A STUDY OF LINEAR FEEDBACK SHIFT REGISTER CIRCUITS OVER GF(2^n)

A Thesis Submitted
In Partial Fulfilment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY

by

SHAKEEL AHMAD

to the

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR
SEPTEMBER 1984

EE-1984-M-AHM-STU

CERTIFICATE

This is to certify that the work "A STUDY OF LINEAR FEEDBACK SHIFT REGISTER CIRCUITS OVER $GF(2^n)^n$ has been carried out by S. Ahmad under my supervision and has not been submitted elsewhere for a degree.

M.U. Siddiqi 24-9-84

September - 1984

(M.U. Siddiqi)
Assistant Professor
Department of Electrical Engineering
Indian Institute of Technology Kanpur
INDIA

ACKNOWLEDGEMENTS

I wish to extend my deep sense of gratitude to Dr. M.U. Siddiqui for his constant encouragement and patience throughout the course of this work.

Thanks are also due to my friends, associates and wellwishers for useful discussions held with them.

At the last, but not the least, I want to thank Mr. S.K. Tewari and Mr. B. Ram for typing and cyclo-styling the thesis.

September 24th, 1984 S. Ahmad

CONTENTS

ABSTRACT

The present thesis is a study of linear feedback shift register circuits (LFSR) over $GF(2^n)$. It is shown that sequences of binary n-tuples can be represented as sequences over $GF(2^n)$ and therefore can be generated by LFSR circuits over $GF(2^n)$. The multiplication of two field elements (binary n-tuples) is shown to be equivalent to multiplication of an appropriately chosen n x n binary matrix corresponding to one of the two elements, by the n x 1 vector corresponding to the other element. A procedure is given to obtain the binary matrices corresponding to field elements. The response of LFSR circuits over $GF(2^n)$ is studied. This includes both the autonomous response and the response to periodic input over $GF(2^n)$. Some of the properties of autonomous response of LFSR circuits over $GF(2^n)$, viewed as n binary sequences put row by row, regarding relationship between these rows, their individual periods and period of overall sequence are described. A synthesis procedure based on Massey's algorithm for designing a LFSR to generate a sequence of binary n-tuples is given. This includes determination of the tap coefficients, the length of the circuit and initial states, such that the number of stages in the LFSR is minimum. A computer program is given which can be used for the design of LFSR by the above procedure. Some of the applications of LFSR circuits and of the synthesis procedure are described.

CHAPTER I

INTRODUCTION

The present thesis is a study of a particular class of linear sequential circuits which are capable of handling sequences of binary n-tuples. Such circuits are basically LSC^S over GF(2^n), in which the field elements are represented by n-tuples formed by binary coefficients of polynomials with degree less than n, and the multiplication and addition of these polynomials is modulo an irreducible polynomial [see chapter 2] of degree n. Thus all the 2^n binary n-tuples $[a_0 a_1 a_2 \cdots a_{n-1}]$, $a_i \varepsilon$ GF(2) are elements of GF(2^n) and are represented by n x 1 vectors.

The block diagram of a general LSC is shown in Fig. 1.1. It consists of a number of synchronous delays which are fed in by various linear combinations of the contents of the delays, and in addition, by the external inputs. The outputs are also combinations of the similar type. The contents of the delays, called state variables, and the outputs at any instant are given by the following matrix equations:

$$\underset{\sim}{X}(k+1) = \underset{\approx}{A}\underset{\sim}{X}(k) + \underset{\approx}{B}\underset{\sim}{U}(k)$$

$$\underset{\sim}{Y}(k) = \underset{\approx}{C}\underset{\sim}{X}(k) + \underset{\approx}{D}\underset{\sim}{U}(k)$$

where the vectors $\underset{\sim}{X}, \underset{\sim}{U}$ and $\underset{\sim}{Y}$ denote the states, inputs and outputs respectively, and $\underset{\approx}{A}, \underset{\sim}{B}, \underset{\sim}{C}$ and D are matrices of compatible dimensions.

When the matrices $\underset{\approx}{A}$ and $\underset{\sim}{B}$ are of the type:

$$\underset{\approx}{A} = \begin{bmatrix} c_1 & c_2 & c_3 & \cdots\cdots & c_{m-1} & c_m \\ 1 & 0 & 0 & \cdots\cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \cdots\cdots & 1 & 0 \end{bmatrix} \quad ; \quad \underset{\sim}{B} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

then the circuit becomes of the type shown in Fig. 1.2 and is called a linear feedback shift register (LFSR) circuit. When a sequence $U^{(k)}$ is fed to the circuit, the output $Y^{(k)}$ becomes a linear combination of the states $X_1^{(k)}, X_2^{(k)} \ldots X_m^{(k)}$ and the input $U^{(k)}$, and a sequence is obtained at the output. Generally the matrices C and D are of the form

$$\underset{\sim}{C} = [\, c_1 \; c_2 \; c_3 \; \cdots\cdots \; c_m \,] \; ; \; D = 1 \; .$$

Sometimes $\underset{\sim}{C} = [000\ldots1]$ and $D = 0$ or other choices are used. For these two choices, the outputs Y and Y' are shown in the figure. The constants $c_1, c_2, c_3 \ldots c_m$ are called tap coefficients. When the entries of the matrices $\underset{\approx}{A}, \underset{\sim}{B}, \underset{\sim}{C}$ and D are from some finite field $GF(q)$, where $q = p^n$, (p is prime) and the circuit is capable of handling data from $GF(q)$, the circuit is called LFSR circuit over $GF(q)$.

Design of LFSR circuits is simpler than that of a general LSC and LFSR circuits have got a wide range of

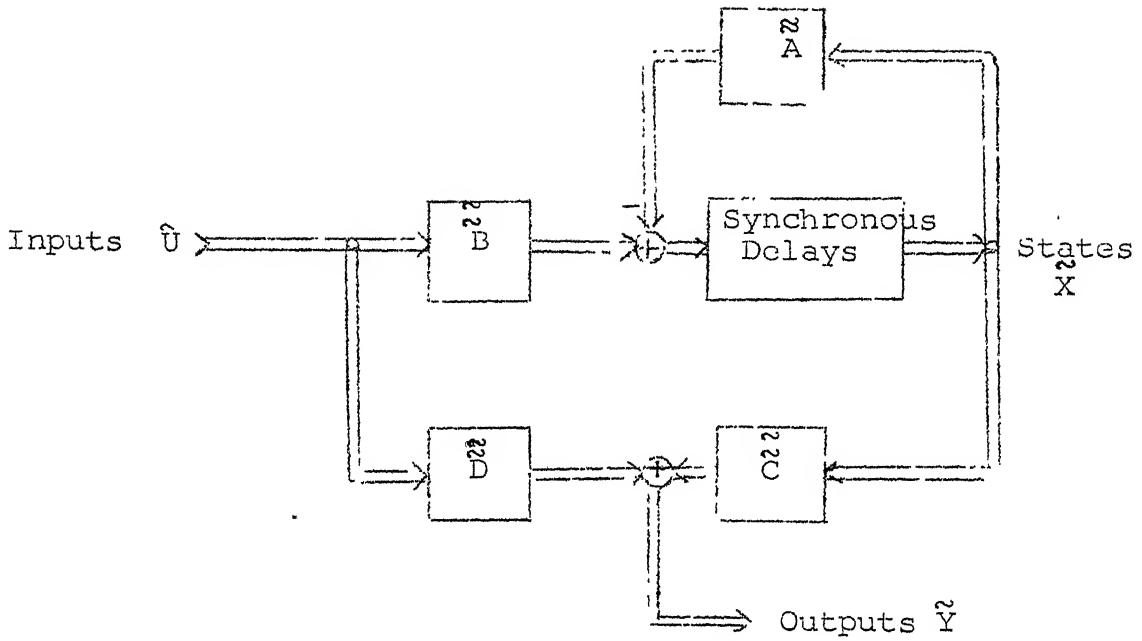


Fig.1.1 Block Diagram of a General LSC

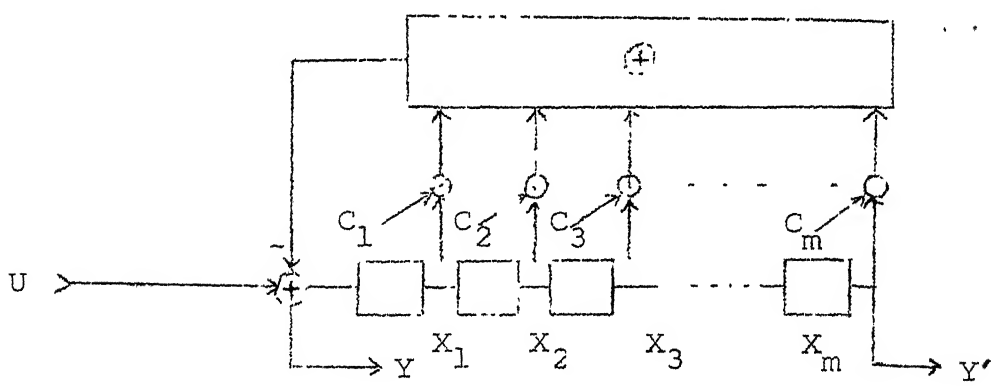


Fig.1.2. A General LFSR Circuit

applications. Properly designed LFSR circuits can translate a sequence into another with desired properties like extension of period etc. and thus are useful for scrambling, cryptography and BCH decoding etc.

In this thesis, we study LFSR circuits over $GF(2^n)$ where elements of the field are represented by binary vectors. The structure of such circuits, their autonomous response properties of autonomous response and their response to periodic inputs are studied.

The synthesis of such circuits is also studied in this thesis. This study involves the design of LFSR circuits which can generate a given vector sequence. The connection polynomial and the shift register length are the two things to be determined in the design. However, since the LFSR circuit which can generate a given sequence is not unique, a procedure is also given to choose the one which has got minimum number of stages.

Historical Background: - The concept of linear sequential networks was originally described by Huffman[1] and since then several generalisations have been suggested[2]. Huffman suggested that the results obtained for binary case are still valid if the polynomials describing the circuits are based on some number system other than binary. Elpas[3], Hartmanis[4] and many others have considered the linear modular sequential circuits over $GF(p)$, $p > 2$ and prime, as generalisation of binary case. Friedland and Stern[6] have

considered such circuits whose state variables and input and output data are vector representation of elements of $GF(p^r)$. In the generalisation of such circuits, the multiplication of a vector by another vector modulo*$[p,q(x)]$ is represented by a matrix-vector multiplication. Then they have proved that a k^{th} order LMSC over $GF(p^r)$ is equivalent to a $(k.r)^{th}$ order LMSC over $GF(p)$, and since synthesis procedure for systems having a prime number of levels are known, the circuit can be synthesized. However, they have not given the details of how the LMSC over $GF(p^r)$ can be obtained from the equivalent $(kr)^{th}$ order LMSC over $GF(p)$. Nakamura and Idawere[7] have discussed multilevel pulse sequence scramblers, in which the data are elements of $GF(2^n)$. Massey[8] has given a LFSR circuit synthesis algorithm which is modification of Berlekamp's iterative algorithm[9] for error correction which is applicable to sequences from any finite field. However the synthesis procedure for sequences consisting of n-tuples in particular is not studied yet.

Organisation of the Thesis: - Chapter 2 gives relevant results concerning finite fields and their representation by polynomials, n-tuples and matrices. Representation of sequence using d-operator is also described.

In chapter 3, expressions for the response of vector LFSR circuits are described. These include both the autonomous

* Details will appear in chapter 2

response, and the response to periodic input sequences. Some properties of autonomous response sequences, viewed as a bank of n binary sequences put row by row, are derived. It is shown that how a sequence generated by a LFSR circuit having some connection polynomial is related to another, generated by a LFSR circuit whose connection polynomial is related to earlier one in a particular manner. Circuits generating maximal sequences are analysed. Expression for period of output sequences in terms of input sequence period is also given.

Chapter 4 describes a design procedure for a LFSR circuit (including the calculation of connection polynomial, shift register length and initial states) which can generate a given sequence of n-tuples. The synthesis procedure is based upon Massey's algorithm. Appropriate flow charts are given to explain the overall synthesis procedure, and the Massey's algorithm. Finally a computer program is given which is used for LFSR circuit synthesis. Illustrative examples are also included.

The thesis is concluded in chapter 5, in which results obtained are discussed and problems for further investigations are given.

Application of LFSR circuits:- A LFSR circuit translates a periodic sequences into another with some desired properties which can be achieved by proper design

of LFSR circuit and thus can be used in places where some sequence is converted into another with some desired properties like extension of period or insertion of frequent transitions. A few of its applications are described here.

One of the most important applications of LFSR circuits is scramblers. Scramblers [5] are digital machines which translate a periodic data sequence into another with much extended period. This operation is most conveniently obtained by adding bit by bit, a maximal sequence to the given sequence. Following factors are responsible for the use of scramblers in a digital data transmission system.

The frequency spectrum of a periodic digital data contains discrete lines. If such signal is to be transmitted through one of channels of a group modulation system, some nonlinearity in the devices may give rise to harmonics of frequencies at which discrete lines exist. These harmonics may fall in the domain of adjacent channel and therefore single tone interference arises. Since tones (discrete lines) are generated in data transmission systems by periodic sequences, and their amplitudes are inversely proportional to period, a larger period is desirable.

Recovery of clock from the digital data is one of the major operations done by the receiver equipments. The clock is recovered using circuits which operate with zero crossings in the received data. Therefore if the transmitted data

contains a string of '1's only or '0's only, then the performance of clock recovery circuit will degrade. Also if the transmitted data is periodic with small period, its frequency spectrum will contain discrete lines at frequencies different from clock frequency. Thus the clock may get locked to some other frequency giving rise to timing error.

From the above reasons, we conclude that the transmitted data must contain sufficient number of level transitions and should not have periodic data with small period. This is achieved by use of scramblers[10].

Scramblers, alongwith lengthening of data period, also do one more important operation, viz. systematic jitter suppression[10]. Timing jitter is the phase modulation of received signal due to some oblitcrations in zero crossings of received signal. This get accumulated at every repeater stage and leads to crosstalk and distortion. The timing jitter related to pulse train is called systematic jitter and is mainly due to ISI, finite pulse width and clock threshold offsets. This can considerably be reduced by incorporating scramblers[11].

Another application of LFSR circuits is encryption in which a digital data is translated into another by adding to it, bit by bit, a sequence. We will see later that this is achieved by possing the data through a LFSR circuit. However if a m-sequence is simply added to data, this

encryption is not secure and can be decoded by a hit and trial method[12,13]. If some nonlinear but reversible operation is done with the data using sequences of high complexity the decoding becomes very difficult and can not be done easily by hit and trialmethod. Generation of such sequences with higher complexity is described by Kalouptsidis and Mandarakis[14].

The LFSR synthesis algorithm has got a very important application in decoding of BCH codes. BCH codes[9] are cyclic codes whose generator polynomial $g(x)$ is chosen to be a minimum degree polynomial with coefficients in $GF(p)$ having $\alpha^{m_o}, \alpha^{m_o+1}, \ldots \alpha^{m_o+d-2}$ as roots, where α is a specified nonzero element of $GF(p^m)$, m_o is a positive integer and d is an integer larger than 2 such that $d-1$ specified roots of $g(x)$ are all distinct. This code has length n, distance d and code redundancy r, where n is exponent of $g(x)$ and r is its degree.

If a BCH code, described by the polynomial $f(x) = f_o+f_1x+\ldots+\ldots+f_{n-1}x^{n-1}$ is transmitted and the received vector $r(x)$ has some errors, then the weighted power sum symmetric function S_i, associated with the error polynomial $e(x) = r(x)-f(x)$ is defined as

$$S_i = e(\alpha^i) \qquad i=1,2,3\ldots$$

and therefore $$S_i = r(\alpha^i) \qquad i=m_o, m_o+1 \ldots m_o\ d-2$$

If t errors occur then e(x) has t nonzero components. If j^{th} nonzero component of e(x) is the digit e_k then $X_j = \alpha^k$ is called the error locator and $Y_i = e_k$ is the error magnitude and these are related to S_i as

$$S_i = \sum_{j=1}^{t} Y_j X_j^i \qquad i=1,2,3\ldots$$

Forney[15] has shown that Y_j can be determined from the knowledge of X_j. Thus the essential BCH decoding problem reduces to determination of X_j, j=1,2,...t, knowing S_i, $i=m_o, m_o+1 \ldots m_o+d-2$

It has been shown by Berkkamp[9] and Massey[8] that

$$S_{m_o} + S_{m_o+1}\, d + S_{m_o+2}\, d^2 + \ldots + \ldots = \frac{p(d)}{c(d)} ,$$

where d is the delay operator

and $$p(d) = \sum_{j=1}^{t} Y_j X_j^{m_o} \prod_{\substack{k=1 \\ k\neq j}}^{t} (1-X_k d)$$

and $$c(d) = \prod_{j=1}^{t} (1-X_j d)$$

and c(d) is the connection polynomial of a unique shortest LFSR over $GF(p^m)$ that generates the sequence $S_{m_o}, S_{m_o+1} \ldots S_{m_o+d-2}$. The roots of c(d) are reciprocals of the t error locators.

Thus knowing the S_i obtained from the received vector, we can design a LFSR which generates the sequence S_i, $i=m_o, m_o+1 \ldots$ and the roots of the connection polynomial of this LFSR can be used to find the error locators[16] and hence the errors.

CHAPTER II

MATHEMATICAL PRELIMINARIES

This chapter includes relevant text on algebra of galois fields and representation of field elements by polynomials, n-tuples and matrices. The set of all binary n-tuples also represents set of elements of $GF(2^n)$ and has a one-to-one correspondence with set of binary polynomials of degree less than n. The multiplication of n-tuples is equivalent to multiplication of an appropriately chosen n x n binary matrix by a n x 1 vector. The procedure to obtain these matrices, given by Friedland and Stern[6] is explained in this chapter, and an alternative procedure is also given. Representation of sequences using d-operator, and their representation by polynomials in d is also described. Since adequate literature is available on these topics, relevant results are quoted in this chapter without proof, details can be seen in the references [17] through [20].

2.1 Finite Fields and Extensions:- In this section, definitions of finite field, extension of finite field and other relevant terms are given and the representation of elements of extension field by polynomials is described.

2.1-1 Finite Fields

A finite field is defined as an algebraic structure consisting of a finite set S alongwith two binary operations $\oplus$ and $\odot$, such that $<S, \oplus>$ is an abelian group under addition, and the set of all nonzero elements of S, alongwith the operation $\odot$ forms a cyclic multiplicative group, and $\odot$ distributes over $\oplus$.

The operations $\oplus$ and $\odot$ are known as field addition and multiplication operations, and are generally different from ordinary operations. Field is denoted by $<S, \oplus, \odot>$.

Finite fields are also called modular fields or galois fields, and are written as GF(q), where q is the number of elements in the field. 'q' has to be either a prime number, or some integral power of a prime number i.e. $q = p^n, n=1,2,3...$ and p is prime.

A number of mathematical structures may be used to represent the elements of a field. If two fields are such that they have equal number of elements, and there is a one to one mapping φ between the elements of the two fields say F_1 and F_2 such that

$$\varphi(a \oplus b) = \varphi(a) \Delta \varphi(b)$$
$$\varphi(a \odot b) = \varphi(a) \circ \varphi(b)$$

for all $a,b \in F_1$ with field operations $\oplus$ and $\odot$ and $\varphi(a), \varphi(b) \in F_2$ with field operations Δ and $\circ$

then the two fields are said to be isomorphic. In this thesis, all isomorphic fields having q elements will be denoted by GF(q). When n=1, it is very convenient to represent the elements of the field GF(p) by the integers 0,1,2,...p-1, and to define the operations $\oplus$ and $\odot$ as,

$$a \oplus b = \begin{cases} a+b & a+b < p \\ a+b-p & a+b \geq p \end{cases} \qquad 2.1\text{-}1$$

$$a \odot b = \begin{cases} a.b & a.b < p \\ a.b-pi & pi \leq a.b < p(i+1) \end{cases} \qquad 2.1\text{-}2$$

where a and b are elements of the field and '+' and '.' are ordinary addition and multiplication operations. This field has p elements and is written as GF(p). The operation $\oplus$ is called addition modulo-p.

Example 2.1 Consider GF(2). The elements are represented by 0 and 1.

Then $0 \oplus 0 = 0 + 0 = 0$; $0 \odot 0 = 0 \times 0 = 0$

$0 \oplus 1 = 0 + 1 = 1$; $0 \odot 1 = 0 \times 1 = 0$

$0 \oplus 0 = 1 + 0 = 1$; $1 \odot 0 = 1 \times 0 = 0$

$1 \oplus 1 = 1 + 1 = 1+1-2-0$; $1 \odot 1 = 1 \times 1 = 1$

2.1-2 Field Extensions:-

Consider a set T having p^n elements where p is a prime number and n=2,3,4... . Let # and * be two binary operations such that $<T, \#, *>$ is a field. Let S be a subset of T having p elements and $<S, \#, *>$ be a field isomorphic to

to GF(p). Then the field $<T, \#, * >$ is said to be an extension of $<S, \#, * >$ 'n' is called degree of extension.

The n^{th} degree extension of GF(p) is written as $GF(p^n)$.

Now we shall see how $GF(p^n)$ can be formed from GF(p). For this, following definitions are useful.

A polynomial $q(x) = q_0 + q_1 x + q_2 x^2 + \ldots + \ldots + q_{n-1} x^{n-1} + q_n x^n$ over a field GF(p) {i.e. the coefficients q_i are from GF(p)} is said to be reducible over this field if it can be written as a product of two polynomials over GF(p). Otherwise it is said to be irreducible.

The exponent of a polynomial is defined as the least integer e such that the polynomial is factor of $1-x^e$.

An irreducible polynomial of degree n over GF(p) is said to be primitive if its exponent is q^n-1. Now consider the set of all polynomials over GF(p), with degree less than n.

i.e. $T = \{(a_0 + a_1 x + \ldots + \ldots + a_{n-1} x^{n-1}) / a_i \in GF(p),\ i=0,1,2 \ldots n-1\}$

and let $q(x) = q_0 + q_1 x + q_2 x^2 + \ldots + \ldots + q_{n-1} x^{n-1} + x^n$ 2.1-3

be an irreducible polynomial of degree n over GF(p).

Then $< T, \#, * >$ is defined as the n^{th} degree extension of GF(p) and is written as $GF(p^n)$, where the field operations # and * are defined by

$$A(x) \# B(x) = \sum_{i=0}^{n-1} (a_i \oplus b_i) x^i \qquad 2.1\text{-}4$$

$$A(x) * B(x) = \sum_{i=0}^{2n-2} \sum_{j=0}^{i} (a_j \odot b_{i-j}) x^i \bmod q(x) \qquad 2.1\text{-}5$$

where $A(x) = \sum_{i=0}^{n-1} a_i x^i \in T$

$B(x) = \sum_{i=0}^{n-1} b_i x^i \in T$

$a_i, b_i \in GP(p)$

$\oplus$ and $\odot$ are GF(p) operations

and mod q(x) means whenever power of x exceeds n-1, x^n is replaced by $x^n - q(x)$, where q(x) is given by 2.1-3. Thus RHS of 2.1-5 is a polynomial of degree less than n and therefore is an element of T.

It can be verified that the set S of all polynomials of degree zero over GF(p) is a subset of T and $< S, \#, * >$ is a field isomorphic to GF(p). Therefore $< T, \#, * >$ is an n^{th} degree extension of GF(p). The operations # and * are called addition and multiplication modulo [p, q(x)]

2.1-3 Representation of field elements by power of primitive element:

An element of a field GF(q) is said to be a primitive element of the field if it can generate all other nonzero elements of the field by repeated multiplication of itself.

The order of a field element is defined as the least integer, to which the element should be raised to get the unit

element of the field. Thus if α is a field element and $\alpha^v = 1$, $\alpha^k \neq 1$ for $k < v$ then v is the order of α.

The order of a primitive element of GF(q) is $q-1$. i.e. $\alpha^{q-1} = 1$

In any field isomorphic to GF(q), there are a number of primitive elements. One of them is represented by some symbol α. Then others are written as $\alpha^2, \alpha^3 \ldots \alpha^{q-1}$.

Example 2.2. Consider the field $GF(2^4)$. Here p=2, n=4. Let $q(x) = 1+x+x^2+x^3+x^4$ be an irreducible polynomial over GF(2).

Then $T = \{1, x, x^2, x^3, 1+x, 1+x^2, 1+x^3, x+x^2, x+x^3, x^2+x^3, 1+x+x^2,$
$1+x+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3, 0\}$

We see that the polynomials $1+x+x^2, 1+x+x^3, x+x^3, 1+x^2, x+x^2, 1+x, 1+x^3, x+x^2+x^3$ have order 15 and therefore can be chosen as primitive elements. Choosing $x+x^2$ as primitive element and denoting it by α, the others can be obtained by repeated multiplication of $x+x^2$ by itself in a manner defined by 2.1-5. Thus

$1 = 1$

$\alpha = x+x^2$

$\alpha^2 = (x+x^2) * (x+x^2)$

$= x^2 + x^4$

$= x^2 + (x^4 - (1+x+x^2+x^3+x^4)$

$= x^2+1+x+x^2+x^3 = 1+x+x^3$

$$\begin{aligned}
\alpha^3 &= (1+x+x^3) * (x+x^2) \\
&= x+x^3+x^4+x^5 \\
&= x+x^3+(x^4-1-x-x^2-x^3-x^4) \\
&\qquad +(x^4-1-x-x^2-x^3-x^4) \\
&= x+x^3+1+x+x^2+x^3 \\
&\qquad +x+x^2+x^3+x^4 \\
&= 1+x+x^3+(x^4-1-x-x^2-x^3-x^4) = \quad x^2
\end{aligned}$$

and we can proceed in a similar manner to get

$$\begin{aligned}
\alpha^4 &= 1+x+x^2 \\
\alpha^5 &= 1 \quad +x^2+x^3 \\
\alpha^6 &= 1+x+x^2+x^3 \\
\alpha^7 &= 1+x \\
\alpha^8 &= \quad x \quad -x^3 \\
\alpha^9 &= \quad x \\
\alpha^{10} &= \quad +x^2+x^3 \\
\alpha^{11} &= 1 \qquad +x^3 \\
\alpha^{12} &= \qquad\quad x^3 \\
\alpha^{13} &= \quad x+x^2+x^3 \\
\alpha^{14} &= 1 \quad +x^2 \\
\alpha^{15} &= 1
\end{aligned}$$

2.2 Other Representations of Field Elements: Mathematical structures other than polynomials are also used to represent the elements of GF(q). In this section, we show that vectors and matrices may also be used to represent elements of GF(q).

Let T be the set of all polynomials over GF(p) with degree less than n-1, as defined in previous section. Let V be the set of all n x 1 vectors with elements from GF(p). Define a mapping φ from V to T as

$$\varphi : \begin{bmatrix} a_o \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \rightarrow (a_o + a_1 x + \ldots + a_{n-1} x^{n-1})$$

where $\begin{bmatrix} a_o \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} \varepsilon$ V and $a_o + a_1 x + \ldots + a_{n-1} x^{n-1} \varepsilon$ T.

It is obvious that this mapping is one to one, and each element of V maps to a unique element of T. The mapping is invertible, and the element of V corresponding to some element of T can be obtained as,

$$\varphi^{-1} (b_o + b_1 x + \ldots + b_{n-1} x^{n-1}) = \begin{bmatrix} b_o \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} \quad \varepsilon \text{ V}$$

The elements of the set of vectors V can be added and multiplied by adding or multiplying the corresponding elements of T and converting them into vectors i.e.

$$\underline{v}_1 \# \underline{v}_2 = \varphi(\varphi^{-1}(\underline{v}_1) \# \varphi^{-1}(\underline{v}_2))$$

$$\underline{v}_1 * \underline{v}_2 = \varphi(\varphi^{-1}(\underline{v}_1) * \varphi^{-1}(\underline{v}_2)) \qquad 2.2\text{-}1$$

Then we see that the set of all n x 1 vectors over GF(p) can represent the elements of GF(q). Now we shall find the procedure to add and multiply these vectors.

Let $\underline{A} = \begin{bmatrix} a_o \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}$ and $\underline{B} = \begin{bmatrix} b_o \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix}$ be two elements of V.

then their sum can be obtained by the procedure given by 2.2-1. Since

$$\varphi^{-1}(\underline{A}) = a_o + a_1 x + \ldots + a_{n-1}x^{n-1} = \sum_{i=0}^{n-1} a_i x^i = A(x)$$

$$\varphi^{-1}(\underline{B}) = b_o + b_1 x + \ldots + b_{n-1}x^{n-1} = \sum_{i=0}^{n-1} b_i x^i = B(x)$$

$$\therefore \varphi^{-1}(\underline{A}) \# \varphi^{-1}(\underline{B}) = A(x) \# B(x)$$

$$= \sum_{i=0}^{n-1} (a_i + b_i)x^i \quad \text{using 2.1-4}$$

$$\therefore \underline{A} \# \underline{B} = \varphi(A(x) \# B(x))$$

$$= \varphi((a_o \oplus b_o) + (a_1 \oplus b_1)x + \ldots + \ldots + (a_{n-1} \oplus b_{n-1})x^{n-1})$$

$$= \begin{bmatrix} a_o \oplus b_o \\ a_i \oplus b_1 \\ \vdots \\ a_{n-1} \oplus b_{n-1} \end{bmatrix}$$

or

$$\begin{bmatrix} a_o \\ a_1 \\ \vdots \\ a_i \\ \vdots \\ a_{n-1} \end{bmatrix} \# \begin{bmatrix} b_o \\ b_1 \\ \vdots \\ b_i \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} a_o \oplus b_o \\ a_1 \oplus b_1 \\ \vdots \\ a_i \oplus b_i \\ \vdots \\ a_{n-1} \oplus b_{n-1} \end{bmatrix} \qquad 2.2\text{-}2$$

The multiplication of two vectors can be achieved by the procedure given by the following lemma.

Lemma 2.1. The multiplication of two vectors from the set of n x 1 vectors corresponding to set of polynomial of degree n-1 is equivalent to multiplication of a n x n matrix corresponding to one of the vectors by the other vector.

Proof. The multiplication of A and B can be done by the procedure given by 2.2-1. For this, we first multiply corresponding polynomials

$$A(x) * B(x) = \sum_{i=0}^{2n-2} \sum_{j=0}^{i} (a_j \odot b_{i-j}) x^i \bmod q(x) \text{ using } 2.1\text{-}5$$

The product $A(x) * B(x)$ includes terms having powers of x higher than n-1 which are to be reduced modulo $q(x)$. For this, we write using 2.1-3

$$x^n = -q_o - q_1 x - q_2 x^2 - \ldots\ldots - q_{n-1} x^{n-1}$$

$$x^{n+1} = -q_o x - q_1 x^2 - \ldots\ldots - q_{n-2} x^{n-1} - q_{n-1} x^n$$

$$= -q_o x - q_1 x^2 - \ldots\ldots - q_{n-2} x^{n-1}$$

$$+ q_o q_{n-1} + q_1 q_{n-1} x + q_2 q_{n-1} x^2 + \ldots + \ldots + q_{n-1}^2 x^{n-1}$$

$$= (q_o q_{n-1}) + (q_1 q_{n-1} - q_o) x + (q_2 q_{n-1} - q_1) x^2 + \ldots + \ldots +$$

$$(q_{n-1}^2 - q_{n-2}) x^{n-1}$$

In otherwords we can write

$$x^n = Q_o^{(n)} + Q_1^{(n)} x + Q_2^{(n)} x^2 + \ldots + \ldots + Q_{n-1}^{(n)} x^{n-1}$$

$$x^{n+i} = Q_o^{(n+i)} + Q_1^{(n+i)} x + Q_2^{(n+i)} x^2 + \ldots + \ldots + Q_{n-1}^{(n+i)} x^{n-1}, \quad i=1,2,3,\ldots$$

where the coefficient $Q_j^{(n+i)}$ are given by the recursive equation 2.2-3

$$Q_j^{(n+i+1)} = Q_{j-1}^{(n+i)} - q_j Q_{n-1}^{(n+i)}, \quad j=1,2,\ldots n-1$$

$$Q_o^{(n+i+1)} = - q_o Q_{n-1}^{(n+i)} \qquad 2.2.4$$

and $Q_j^{(n)} = -q_j$

Therefore x^n, x^{n+1}, x^{n+2} ...etc. can be written in terms of n-1 degree polynomials in x. We can write $x^n, x^{n+1}, x^{n+2} \ldots x^{2n-2}$ in terms of $x, x^2 \ldots x^{n-1}$ as the following matrix equation

$$[x^n \; x^{n+1} \; x^{n+2} \ldots \; x^{2n-2}] = [1 \; x \; x^2 \ldots \; x^{n-1}] \cdot \begin{bmatrix} Q_o^{(n)} & Q_o^{(n+1} & \ldots Q_o^{(2n-2)} \\ Q_1^{(n)} & Q_1^{(n+1} & Q_1^{(2n-2)} \\ Q_2^{(n)} & Q_2^{(n+1} & Q_2^{(2n-2)} \\ \vdots & \vdots & \vdots \\ Q_{n-1}^{(n)} & Q_{n-1}^{(n+1)} & Q_{n-1}^{(2n-2)} \end{bmatrix}$$

2.2-5

where the coefficients $Q_j^{(n+i)}$ are given by 2.2-4.

Now we can write

$$A(x) * B(x) = \sum_{i=0}^{2n-2} \sum_{j=0}^{i} (a_j \odot b_{i-j}) x^i \bmod q(x)$$

$$= [1 \; x \; x^2 \ldots x^{n-1} \; \vdots \; x^{n+1} \ldots x^{2n-2}]$$

$$\times \begin{bmatrix} a_0 & 0 & \ldots & 0 & 0 \\ a_1 & a_0 & \ldots & 0 & 0 \\ a_2 & a_1 & \ldots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{n-1} & a_{n-2} & \ldots & a_1 & a_0 \\ 0 & a_{n-1} & \ldots & a_2 & a_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & a_{n-1} \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix} \bmod q(x)$$

$$= [1 \; x \; x^2 \ldots x^{n-1}] \cdot \begin{bmatrix} a_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ldots & 0 \\ a_2 & a_1 & \ldots & 0 \\ \vdots & & & \\ a_{n-1} & a_{n-2} & \ldots & a_0 \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix}$$

$$+ [x^n \; x^{n+1} \ldots x^{2n-2}] \begin{bmatrix} 0 & a_{n-1} & \ldots & a_1 \\ 0 & 0 & \ldots & a_2 \\ \vdots & & & \\ 0 & 0 & \ldots & a_{n-1} \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} \bmod q(x)$$

$$=[1x\ x^2 \ldots\ x^{n-1}]\left\{\begin{bmatrix} a_o & 0 & \ldots & 0 \\ a_1 & a_o & \ldots & 0 \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ a_{n-1} & a_{n-2} & \ldots & a_o \end{bmatrix} + \begin{bmatrix} Q_o^{(n)} & Q_o^{(n+1)} & \ldots & Q_o^{(2n-2)} \\ Q_1^{(n)} & Q_1^{(n+1)} & \ldots & Q_1^{(2n-2)} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{n-1}^{(n)} & Q_{n-1}^{(n+1)} & & Q_{n-1}^{(2n-2)} \end{bmatrix}\right\} \times \left\{\begin{bmatrix} 0 & a_{n-1} & \ldots & a_1 \\ 0 & 0 & \ldots & a_2 \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ 0 & 0 & \ldots & a_{n-1} \end{bmatrix}\cdot\begin{bmatrix} b_o \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{bmatrix}\right\} \qquad 2.2\text{-}6$$

$$=[1\ x\ x^2 \ldots\ x^{n-1}]\begin{bmatrix} a'_{oo} & a'_{o1} & \ldots & a'_{on-1} \\ a'_{1o} & a'_{11} & \ldots & a'_{1n-1} \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ \cdot & \cdot & & \\ a'_{n-1,o} & a'_{n-1,1} & \ldots & a'_{n-1,n-1} \end{bmatrix}\cdot\begin{bmatrix} b_o \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{bmatrix}$$

and therefore

$$\underline{A} * \underline{B} = \begin{bmatrix} a_o \\ a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_{n-1} \end{bmatrix} * \begin{bmatrix} b_o \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} a'_{oo} & a'_{o1} & \ldots \\ a'_{1o} & a'_{11} & \ldots \\ \cdot & \cdot & \\ \cdot & \cdot & \\ a'_{n-1,o} & a'_{n-1,1} & \ldots \end{bmatrix}\cdot\begin{bmatrix} b_o \\ b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_{n-1} \end{bmatrix} = \underline{\underline{A}} \cdot \underline{B} \qquad 2.2\text{-}7$$

where the matrix $\underline{\underline{A}} = [a'_{ij}]$ on the RHS of above equation is the matrix appearing in the bracket in the RHS of Eq. 2.2-6.

Thus we see that multiplication of two vectors is equivalent to multiplication of a n x n matrix whose elements depend upon the elements of $\underline{A}$ and coefficients of $q(x)$, by the other vector. However computation of the above matrix $\underline{A}$ by this procedure is quite involved and we give a simple procedure to compute this matrix after the following example.

Example 2.3. Multiply $\underline{A} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ and $\underline{B} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$,

given $q(x) = 1+x+x^2+x^3+x^4$.

The equation $1+x+x^2+x^3+x^4 = 0$ gives

$$x^4 = 1+x+x^2+x^3$$

$$\therefore \quad x^5 = x*(1+x+x^2+x^3) = x+x^2+x^3+x^4 = x+x^2+x^3+1+x+x^2+x^3$$

$$= 1$$

$$x^6 = x$$

Therefore

$$[x^4 \; x^5 \; x^6] = [1 \; x \; x^2 \; x^3] \cdot \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\therefore \quad A(x) * B(x) = [1 \quad x \quad x^2 \quad x^3] \cdot \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$+ \begin{bmatrix} x^4 & x^5 & x^6 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x & x^2 & x^3 \end{bmatrix} \cdot \left\{ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x & x^2 & x^3 \end{bmatrix} \cdot \left\{ \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \right\} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x & x^2 & x^3 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x & x^2 & x^3 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

and therefore

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} * \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Recall for Ex.2.2 that $\underline{A} = \alpha$, $\underline{B} = \alpha^6$ and therefore $\underline{A} * \underline{B} = \alpha^7$. Therefore result is verified .

Procedure to obtain the matrices corresponding to vectors:

It has been shown in previous section that the multiplication of two vectors is equivalent to multiplication of a matrix corresponding to one of the vectors by the other. Now we give two alternative procedures to determine the matrix corresponding to a given vector. The first procedure is the one described by Friedland and Stern[6]. Then another procedure is given and it is proved that the matrices obtained by both cases are the same.

Let $A(x)$ and $B(x)$ be two polynomials of degree n-1 and $\underline{A}$ and $\underline{B}$ be corresponding vectors. The product of $A(x)$ and $B(x)$ can be written as

$$C(x) = A(x)\,B(x) = (a_o + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}).B(x)$$

$$= a_o.B(x) + a_1.x.B(x) + a_2 x^2.B(x) + \ldots + \ldots + a_{n-1} x^{n-1}.B(x)$$

Writing $C(x)$ and $B(x)$ in vector form, we get,

$$\underline{C} = a_o \underline{B} + a_1 x \underline{B} + a_2 x^2 \underline{B} + \ldots + \ldots + a_{n-1} x^{n-1} \underline{B} \qquad 2.2\text{-}8$$

where $\underline{B}$ is representing the polynomial $b_o + b_1 x + b_2 x^2 + \ldots + b_{n-1} x^{n-1}$. If the multiplication is modulo-$q(x)$, x^n is replaced by $x^n - q(x)$ and therefore

$$x.B(x) = b_o x + b_1 x^2 + \ldots + b_{n-2} x^{n-1} + b_{n-1} x^n \bmod q(x)$$

$$= (-q_o b_{n-1}) + (b_o - q_1 b_{n-1})x + (b_1 - q_2 b_{n-1})x^2 + \ldots + \ldots +$$

$$(b_{n-2} - b_{n-1} q_{n-1}) x^{n-1}$$

or in the matrix form,

$$x.\underline{B} = \begin{bmatrix} 0 & 0 & \dots & 0 & -q_0 \\ 1 & 0 & \dots & 0 & -q_1 \\ 0 & 1 & \dots & 0 & -q_2 \\ \cdot & \cdot & & \cdot & \\ \cdot & \cdot & & \cdot & \\ \cdot & \cdot & & \cdot & \\ 0 & 0 & & 1 & -q_{n-1} \end{bmatrix} . \underline{B} = \underline{\underline{M}}.\underline{B} \qquad 2.2\text{-}9$$

Substituting 2.2-9 in 2.2-8, we get

$$\underline{C} = a_0\underline{B} + a_1\underline{\underline{M}}.\underline{B} + a_2\underline{\underline{M}}^2.\underline{B} + \dots + \dots + a_{n-1}\underline{\underline{M}}^{n-1}.\underline{B}$$

$$\text{or} \quad \underline{C} = (a_0\underline{\underline{I}} + a_1\underline{\underline{M}} + a_2\underline{\underline{M}}^2 + \dots + \dots + a_{n-1}\underline{\underline{M}}^{n-1}).\underline{B} = \underline{\underline{A}}.\underline{B}$$

$$\text{where} \quad \underline{\underline{A}} = a_0\underline{\underline{I}} + a_1\underline{\underline{M}} + a_2\underline{\underline{M}}^2 + \dots + \dots + a_{n-1}\underline{\underline{M}}^{n-1} \qquad 2.2\text{-}10$$

$$\text{and} \quad \underline{\underline{M}} = \begin{bmatrix} 0 & 0 & \dots & 0 & -q_0 \\ 1 & 0 & \dots & 0 & -q_1 \\ 0 & 1 & \dots & 0 & -q_2 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & -q_{n-1} \end{bmatrix} \text{(from Eqn. 2.2-9)} \qquad 2.2\text{-}11$$

The matrix $\underline{\underline{M}}$ is the companion matrix corresponding to the polynomial $q(x)$, and using powers of $\underline{\underline{M}}$, the matrix $\underline{\underline{A}}$ corresponding to the vector $\underline{A}$ can be constructed.

Now we give an alternative procedure for construction of $\underline{\underline{A}}$. Let $\underline{\alpha}$ be the primitive element of $GF(p^n)$, where the elements of $GF(p^n)$ are represented by vectors over $GF(p)$. Therefore $\underline{\alpha}$ corresponds to some polynomial say $\alpha_0 + \alpha_1 x + \dots + \alpha_{n-1}x^{n-1}$ and let some power of $\underline{\alpha}$ say $\underline{\alpha}^v$ corresponds to the polynomial x. Therefore

$$\underline{\alpha}^{v} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

and $(\underline{\alpha}^{v})^{i} = \underline{\alpha}^{v\,i}$ corresponds to x^{i} and thus

$$\underline{\alpha}^{2v} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad ; \quad \underline{\alpha}^{3v} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \qquad \underline{\alpha}^{(n-1)v} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \text{ and } \underline{\alpha}^{nv} = \begin{bmatrix} -q_o \\ -q_1 \\ -q_2 \\ \vdots \\ -q_{n-1} \end{bmatrix}$$

since $\underline{\alpha}^{nv}$ corresponds to x^{n} which is equal to

$-q_o - q_1 x - q_2 x^2 \ldots\ldots - q_{n-1} x^{n-1}$.

Now let $\underline{\underline{\alpha}}$ be the matrix corresponding to $\underline{\alpha}$.

Since $\underline{\alpha} * \underline{1} = \underline{\alpha}$ therefore $\underline{\underline{\alpha}} . \underline{1} = \underline{\alpha}$

and similarly $\underline{\alpha} * \underline{\alpha}^{v} = \underline{\alpha}^{v+1}$ therefore $\underline{\underline{\alpha}} . \underline{\alpha}^{v} = \underline{\alpha}^{v+1}$

$\vdots$

$\underline{\alpha} * \underline{\alpha}^{(n-1)} = \underline{\alpha}^{(n-1)v+1}$ therefore $\underline{\underline{\alpha}} . \underline{\alpha}^{(n+1)v} = \underline{\alpha}^{(n-1)v+1}$.

We can verify that all other equations can be represented as linear combinations of the above n equations. The above n equations can be written simultaneously as n columns of the following matrix equation

$$[\underline{\alpha}.\underline{1}\ \underline{\alpha}.\underline{\alpha}^{v}\ \underline{\alpha}\underline{\alpha}^{2v}\ldots\ \ldots\underline{\alpha}.\underline{\alpha}^{(n-1)v}]=[\underline{\alpha}\ \underline{\alpha}^{v+1}\ \underline{\alpha}^{2v+1}\ldots\underline{\alpha}^{(n-1)v+1}]$$

or $$\underline{\alpha}\,[\underline{1}\ \underline{\alpha}^{v}\ \underline{\alpha}^{2v}\ \ldots\ \ldots\underline{\alpha}^{(n-1)v}]\ =[\underline{\alpha}\ \underline{\alpha}^{v+1}\ \underline{\alpha}^{2v+1}\ldots\underline{\alpha}^{(n-1)v+1}]$$

2.2-12

The matrix $[\underline{1}\ \underline{\alpha}^{v}\ \underline{\alpha}^{2v}\ldots\ \ldots\ \underline{\alpha}^{(n-1)v}]$ is the unity matrix and therefore 2.2-12 becomes

$$\underline{\alpha} = [\underline{\alpha}\ \underline{\alpha}^{v+1}\ \underline{\alpha}^{2v+1}\ldots\ \ldots\ \underline{\alpha}^{(n-1)v+1}] \qquad 2.2\text{-}13$$

This is the matrix corresponding to the vector $\underline{\alpha} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}$.

The i^{th} power of this matrix is obtained as follows.

$$\begin{aligned}
\underline{\alpha}^{i} &= \underline{\alpha}^{i-1}\,\underline{\alpha} \\
&= \underline{\alpha}^{i-1}[\underline{\alpha}\ \underline{\alpha}^{v+1}\ \underline{\alpha}^{2v+1}\ldots\ \underline{\alpha}^{(n-1)v+1}] \\
&= \underline{\alpha}^{i-2}[\underline{\alpha}\ \underline{\alpha}\ \underline{\alpha}\ \underline{\alpha}^{v+1}\ \underline{\alpha}\ \underline{\alpha}^{2v+1}\ldots\underline{\alpha}\ \underline{\alpha}^{(n-1)v+1}] \\
&= \underline{\alpha}^{i-2}[\underline{\alpha}^{2}\underline{\alpha}^{v+2}\underline{\alpha}^{2v+2}\ \ \ldots\ \ \alpha^{(n-1)v+2}] \\
&= \ldots
\end{aligned}$$

or $$\underline{\alpha}^{i} = [\underline{\alpha}^{i}\ \underline{\alpha}^{v+i}\ \underline{\alpha}^{2v+i}\ \ \ldots\ \ \underline{\alpha}^{(n-1)v+i}] \qquad 2.2\text{-}14$$

Now let us prove that the i^{th} power of $\underline{\alpha}$ corresponds to i^{th} power of $\underline{\alpha}$ and the two sets $\{\underline{\alpha}\ \underline{\alpha}^{2}\ldots\underline{\alpha}^{q-1}\}$ and $\{\underline{\alpha},\underline{\alpha}^{2}\ldots\ \underline{\alpha}^{q-1}\}$ have a one-to-one correspondence. Suppose $\underline{\alpha}^{i}$ corresponds to $\underline{\alpha}^{i}$ and $\underline{\alpha}^{j}$ corresponds to $\underline{\alpha}^{j}$. Then it is sufficient to prove that $\underline{\alpha}^{i}\,\underline{\alpha}^{j}$ corresponds to $\underline{\alpha}^{i+j}$. Since,

$$\underline{\alpha}^{i} = [\underline{\alpha}^{i}\ \underline{\alpha}^{v+i}\ \underline{\alpha}^{2v+i}\ \ldots\ \underline{\alpha}^{(n-1)v+i}]$$

$$\underline{\alpha}^{j} = [\underline{\alpha}^{j}\ \underline{\alpha}^{v+j}\ \underline{\alpha}^{2v+j}\ \ldots\ \underline{\alpha}^{(n-1)v+j}]$$

and therefore $\underline{\alpha}^{i}\underline{\alpha}^{j} = \underline{\alpha}^{i+j} = [\underline{\alpha}^{i+j}\ \underline{\alpha}^{v+i+j}\ \underline{\alpha}^{2v+i+j}\ldots\underline{\alpha}^{(n-1)v+i+j}]$

which corresponds to $\underline{\alpha}^{i+j} = \underline{\alpha}^{i} * \underline{\alpha}^{j}$

The matrix $\underline{\alpha}$ given by 2.2-13 can further be simplified. Since

$$\underline{\alpha}^{v} = [\underline{\alpha}^{v}\ \underline{\alpha}^{v+v}\ \underline{\alpha}^{2v+v}\ldots\alpha^{(n-1)v+v}] = \begin{bmatrix} 0 & 0 & 0 & \ldots & -q_0 \\ 1 & 0 & 0 & \ldots & -q_1 \\ 0 & 1 & 0 & \ldots & -q_2 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ 0 & 0 & 0 & & -q_{n-1} \end{bmatrix} = \underline{M}$$

(from 2.2-11)

and

$$\underline{\alpha}^{i+j} = \underline{\alpha}^{i} * \underline{\alpha}^{j} = \underline{\alpha}^{i}\ \underline{\alpha}^{j}$$

therefore Eq. 2.2-13 becomes

$$\underline{\alpha} = [\ \underline{\alpha}\ \underline{\alpha}^{v} * \underline{\alpha}\ \ \underline{\alpha}^{2v} * \alpha\ \ldots\ \ \ldots\ \underline{\alpha}^{(n-1)v} * \alpha]$$

$$= [\ \underline{\alpha}\ \underline{\alpha}^{v}\ \underline{\alpha}\ \ \underline{\alpha}^{2v}\ \underline{\alpha}\ \ldots\ \ \ldots\ \underline{\alpha}^{(n-1)v}\ \alpha]$$

or $\underline{\alpha} = [\ \underline{\alpha}\ \underline{M}\cdot\underline{\alpha}\ \ \ \underline{M}^{2}\underline{\alpha}\ \ \ \ldots\ \ \ldots\ \underline{M}^{n-1}\cdot\underline{\alpha}\ ]$ 2.2-15

and therefore Eq. 2.2-14 becomes

$$\underline{\alpha}^{i} = [\ \underline{\alpha}^{i}\ \underline{M}\cdot\underline{\alpha}^{i}\ \underline{M}^{2}\underline{\alpha}^{i}\ \ \ \ldots\ \ \ldots\ \underline{M}^{n-1}\cdot\underline{\alpha}^{i}]$$

or $\underline{A} = [\ \underline{A}\ \ \underline{M}\cdot\underline{A}\ \ \underline{M}^{2}\underline{A}\ \ \ \ldots\ \ \ldots\ \underline{M}^{n-1}\cdot\underline{A}\ ]$ 2.2-16

where $\underline{M}$ is the companion matrix corresponding to irreducible

polynomial $q(x)$ given by 2.2.11 and $\underline{\underline{A}}$ is the matrix equivalent of the vector $\underline{A} = \underline{\alpha}^i$ for any value of i.

Now we prove that the matrix $\underline{\underline{A}}$ given by 2.2-16 is the same as given by 2.2-10 following Friedland and Stern's procedure

Since $\underline{1} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$; $\underline{\alpha}^v = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$ $\underline{\alpha}^{(n-1)v} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$

and similarly $\underline{\alpha}^{nv} = \begin{bmatrix} -q_o \\ -q_1 \\ -q_2 \\ \vdots \\ -q_{n-1} \end{bmatrix} = \begin{bmatrix} Q_o^{(n)} \\ Q_1^{(n)} \\ Q_2^{(n)} \\ \vdots \\ Q_{n-1}^{(n)} \end{bmatrix}$; $\underline{\alpha}^{(n+i)v} = \begin{bmatrix} Q_o^{(n+i)} \\ Q_1^{(n+i)} \\ Q_2^{(n+1)} \\ \vdots \\ Q_{n-1}^{(n+i)} \end{bmatrix}$

$i=1, 2, 3 \ldots .$

where $Q_j^{(n+i)}$ are given by Eq. 2.2-4.

Therefore we can write

$$\underline{\underline{I}} = [\, \underline{1} \;\; \underline{\alpha}^v \;\; \underline{\alpha}^{2v} \;\; \ldots \;\; \underline{\alpha}^{(n-1)v} \,]$$

$$\underline{\underline{M}} = [\, \underline{\alpha}^v \;\; \underline{\alpha}^{2v} \;\; \underline{\alpha}^{3v} \;\; \ldots \;\; \underline{\alpha}^{nv} \,]$$

$$M^2 = \underline{\underline{M}} \cdot [\, \underline{\alpha}^v \;\; \underline{\alpha}^{2v} \;\; \underline{\alpha}^{3v} \ldots \underline{\alpha}^{nv} \,]$$

$$= [\underline{\alpha}^{2v} \;\; \underline{\alpha}^{3v} \;\; \underline{\alpha}^{4v} \;\; \ldots \;\; \underline{\alpha}^{(n+1)v} \,]$$

and similarly higher powers of $\underline{\underline{M}}$ can be written as

$$\underline{\underline{M}}^{i} = [\ \underline{\alpha}^{iv}\ \underline{\alpha}^{(i+1)v}\ \underline{\alpha}^{(i+2)v}\ \ldots\ \underline{\alpha}^{(i+n-1)v}] \qquad 2.2\text{-}17$$

Therefore the matrix $\underline{\underline{A}}$ given by 2.2-10 can be written using Eq. 2.2-19 as,

$$\begin{aligned}\underline{\underline{A}} &= a_o\underline{\underline{I}} + a_1\underline{\underline{M}} + a_2\underline{\underline{M}}^2 + \ldots + \ldots + a_{n-1}\underline{\underline{M}}^{n-1} \\ &= a_o[1\ \ \underline{\alpha}^{v}\ \ \underline{\alpha}^{2v}\ \underline{\alpha}^{3v}\ \ \ldots\ \ \underline{\alpha}^{(n-1)v}] \\ &\quad + a_1[\underline{\alpha}^{v}\ \underline{\alpha}^{2v}\ \underline{\alpha}^{3v}\ \underline{\alpha}^{4v}\ \ \ldots\ \ \underline{\alpha}^{nv}\ \ ] \\ &\quad + a_2[\underline{\alpha}^{2v}\underline{\alpha}^{3v}\ \underline{\alpha}^{4v}\ \underline{\alpha}^{5v}\ \ \ldots\ \ \underline{\alpha}^{(n+1)v}] \\ &\quad + \ldots \\ &\quad + \ldots \\ &\quad + a_{n-1}[\underline{\alpha}^{(n-1)v}\ \underline{\alpha}^{nv}\ \underline{\alpha}^{(n+1)v}\ \underline{\alpha}^{(n+2)v}\ \ \underline{\alpha}^{(2n-2)v}]\end{aligned}$$

The i^{th} colum of the matrix $\underline{\underline{A}}$ is therefore

$$a_o\ \underline{\alpha}^{(i-1)v} + a_1\underline{\alpha}^{iv} + a_2\underline{\alpha}^{(i+1)v} + \ldots + \ldots + a_{n-1}\underline{\alpha}^{(i+n-2)v} \qquad 2.2\text{-}18$$

The i^{th} column of the matrix $\underline{\underline{A}}$ given by Eq. 2.2-16 is

$$\underline{\underline{M}}^{i-1}\underline{\underline{A}} = [\ \underline{\alpha}^{(i-1)v}\ \underline{\alpha}^{iv}\ \underline{\alpha}^{(i+1)v}\ \ldots\ \underline{\alpha}^{(i+n-2)v}]\cdot\underline{\underline{A}}$$

$$= [\ \underline{\alpha}^{(i-1)v}\ \underline{\alpha}^{iv}\ \underline{\alpha}^{(i+1)v}\ \ldots\ \underline{\alpha}^{(i+n-2)v}]\cdot\begin{bmatrix} a_o \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1}\end{bmatrix}$$

$$= a_o\underline{\alpha}^{(i-1)v} + a_1\underline{\alpha}^{iv} + a_2\underline{\alpha}^{(i+1)v} + \ldots + a_{n-1}\ \alpha^{(i+n-2)v}$$

which is the same as given by Eq. 2.2-18 and therefore the matrix $\underline{\underline{A}}$ corresponding to the vector $\underline{A}$ given by both procedures is the same.

The various steps involved in computation of the matrix $\underline{\underline{A}}$ corresponding to some vector $\underline{A}$ are following:

(1) Construct the companion matrix $\underline{\underline{M}}$ corresponding to the given irreducible polynomial $q(x)$

(2) Compute the products $\underline{\underline{M}}\cdot\underline{A}$, $\underline{\underline{M}}^2\underline{A}$ ... $\underline{\underline{M}}^{n-1}\underline{A}$

(3) The matrix $\underline{\underline{A}}$ is given by $\underline{\underline{A}} = [\ \underline{A}\ \underline{\underline{M}}\underline{A}\ \ \underline{\underline{M}}^2\underline{A}\ \ldots\ \underline{\underline{M}}^{n-1}\underline{A}]$

Example 2.4. Find the matrices corresponding to the vectors

$$\underline{A} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \text{ and } \underline{B} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$ using $q(x) = 1+x+x^4$ and find the products $\underline{A} * \underline{B}$ and $\underline{B} * \underline{A}$.

Here $$\underline{\underline{M}} = \begin{bmatrix} 0 & 0 & 0 & -q_0 \\ 1 & 0 & 0 & -q_1 \\ 0 & 1 & 0 & -q_2 \\ 0 & 0 & 1 & -q_3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\underline{\underline{M}}\,\underline{A} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} ; \ \underline{\underline{M}}^2\underline{A} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} ; \ \underline{\underline{M}}^3\underline{A} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

$$\underline{\underline{M}}\,\underline{B} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} ; \ \underline{\underline{M}}^2\underline{B} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} ; \ \underline{\underline{M}}^3\underline{B} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\underline{\underline{A}} = [\, \underline{A} \;\; \underline{\underline{M}}\,\underline{A} \;\; \underline{\underline{M}}^2\underline{A} \;\; \underline{\underline{M}}^3\underline{A} \,] = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\underline{\underline{B}} = [\, \underline{B} \;\; \underline{\underline{M}}\,\underline{B} \;\; \underline{\underline{M}}^2\underline{B} \;\; \underline{\underline{M}}^3\underline{B} \,] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\underline{A} * \underline{B} = \underline{\underline{A}}\,\underline{B} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

$$\underline{B} * \underline{A} = \underline{\underline{B}}\,\underline{A} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Therefore $\underline{A} * \underline{B} = \underline{B} * \underline{A}$ is verified.

From the preceeding discussion, we conclude that the set $\{\underline{A}, \underline{A}^2, \ldots \underline{A}^{q-1}, \underline{\varphi}\}$ of all n x 1 vectors over GF(p) has a one to one correspondence with the set of polynomials and similarly the set $\{\underline{\underline{A}}, \underline{\underline{A}}^2, \ldots \underline{\underline{A}}^{q-1}, \underline{\underline{\varphi}}\}$ of n x n matrices constructed by using 2.2-16 has one to one correspondence with the set of vectors such that $\underline{A}^i$ corresponds to $\underline{\underline{A}}^i$. The multiplication of two vectors is achieved by converting one of them into corresponding matrix using 2.2-16 and multiplying it by the other vector. Thus the set of all n x 1 vectors over GF(p)

alongwith the multiplication and addition operations defined by 2.2-2 and 2.2-7 represents a field isomorphic to $GF(p^n)$. Similarly the set of matrices obtained from the elements of the set of vectors using 2.2-16 alongwith matrix addition and multiplication operations also represents a field isomorphic to $GF(p^n)$.

2.3 Representation of sequences.

A sequence S is an ordered set of elements from some set and is written as $S = s_o s_1 s_2 \cdots$. A sequence is periodic with period P if $s_i = s_{i+kp}$ for all $i=0,1,2,\ldots P-1$ and $k=1,2,3\ldots$. The sequence $T = t_o t_1 t_2 \cdots$ is said to be a shifted version of some sequence $S=s_o s_1 s_2 \cdots$ if for all $i \geq 0$, $t_{i+\beta} = s_i$, and $t_o = t_1 = \cdots = t_{\beta-1} = 0$ where β is some integer. In this case we say that T is equal to S shifted by β bits.

If some sequence $S=s_o s_1 s_2 \cdots$ is delayed by one bit, the delayed sequence can be considered as equal to the sequence S operated upon by a unit delay operator, which is written as d. Thus

$$d\{s_o s_1 s_2 s_3 \cdots\} = \{0 s_o s_1 s_2 \cdots\}$$

Similarly if we denote the infinite sequence

10000..... by δ , where $\delta_o = 1$ and $\delta_{i>o} = 0$

then we can write,

$$10000\ldots = \delta$$

$$01000\ldots = d\delta$$

$$00100\ldots = d^2\delta \quad \text{etc.}$$

and therefore the sequence $S = s_0 s_1 s_2 \ldots$ can be written as,

$$\begin{aligned} S &= s_0 s_1 s_2 s_3 \ldots \\ &= s_0 00000 \ldots \\ &\quad + 0 s_1 0000 \ldots \\ &\quad + 00 s_2 000 \ldots \\ &\quad + 000 s_3 00 \ldots \\ &\quad + \ldots \\ &= s_0\delta + s_1 d\delta + s_2 d^2\delta + s_3 d^3\delta + \ldots + \ldots \end{aligned}$$

$$\text{or} \quad S = (s_0 + s_1 d + s_2 d^2 + s_3 d^3 + \ldots + \ldots + \ldots)\delta$$

$$= S(d)\ \delta$$

This is called the polynomial representation of S. The term δ is generally understood and is omitted. The polynomial $S(d)$ can be obtained by the following equation:

$$S(d) = \sum_{i=0}^{\infty} s_i d^i \qquad 2.3\text{-}1$$

and is called the d-transform of S

If a sequence S is periodic with period P, then it can be written in terms of its d-transform as,

$$S(d) = s_0 + s_1 d + s_2 d^2 + \ldots + \ldots + s_{p-1} d^{p-1} + s_0 d^p + \ldots + \ldots + s_{p-1} d^{2p-1} + s_0 d^p + \ldots$$

$$= (s_0 + s_1 d + s_2 d^2 + \ldots + \ldots + s_{p-1} d^{p-1})(1 + d^p + d^{2p} + \ldots).$$

The polynomial $1+d^p+d^{2p}+\ldots+\ldots$ is a formal geometric series and can be summed up to give

$$1+d^p+d^{2p}+\ldots+\ldots = \frac{1}{1-d^p}$$

since $(1+d^p+d^{2p}+\ldots)(1-d^p) = 1$ and $1-d^p \neq 0$.

Therefore expression for $S(d)$ becomes

$$S(d) = \frac{s_o+s_1d+s_2d^2+\ldots+\ldots+s_{p-1}d^{p-1}}{1-d^p} \qquad 2.3\text{-}2$$

The RHS of above equation may have common factors in numerator and denominator polynomial, and can be cancelled. Therefore we may write,

$$S(d) = \frac{N(d)}{D(d)} .$$

In otherwords, a periodic sequence can be written as a ratio of two polynomials in d.

Suppose $\frac{A(d)}{B(d)}$ be a rational polynomial representing a sequence such that $A(d)$ and $B(d)$ are relatively prime. We know that there exists an integer e such that $B(d)$ is a factor of $1-d^e$ i.e. $B(d)\,B'(d) = 1-d^e$

$$\frac{A(d)}{B(d)} = \frac{A(d).B'(d)}{B(d).B'(d)} = \frac{A'(d)}{1-d^e} .$$

Thus ratio of two relatively prime polynomials in d represent a sequence whose period is equal to exponent of the denominator polynomial.

Example 2.5. Represent the sequence

$S = 01111010110010001111010110010001111\ldots$ over GF(2)

by a rational polynomial. Find $T(d) = d^2S(d)$ and verify that T is a delayed version of S by 2 bits.

Here $S(d) = \sum_{i=0}^{\infty} s_i d^i$

$$= d+d^2+d^3+d^4+d^6+d^8+d^9+d^{12}+d^{16}+d^{17}+d^{18}+d^{19}+d^{21}+d^{23}+d^{24}+d^{27}+\ldots$$

$$= (d+d^2+d^3+d^4+d^6+d^8+d^9+d^{12})(1+d^{15}+d^{30}+\ldots)$$

$$= \frac{d+d^2+d^3+d^4+d^6+d^8+d^9+d^{12}}{1+d^{15}}$$

or $S(d) = \dfrac{d}{1+d+d^4}$

$\therefore$ $T(d) = \dfrac{d^3}{1+d+d^4} = \dfrac{d^3+d^4+d^5+d^6+d^8+d^{10}+d^{11}+d^{14}}{1+d^{15}}$

$\therefore$ $T = 000111101011001000111101010\ldots$

and we see that

$$t_0 = t_1 = t_2 = 0$$

and $$t_{i+3} = s_i, \quad i=0,1,2\ldots .$$

CHAPTER III

LINEAR FEEDBACK SHIFT REGISTER CIRCUITS OVER GF(2^n)

In this chapter, Linear feedback shift register (LFSR) circuits over GF(2^n) are studied. Expressions for the response of LFSR circuits are obtained. It is shown that the response of the LFSR circuit can be viewed as n binary sequences put row by row. Properties of the autonomous response of LFSR circuit regarding periods of individual rows, and their relationship to the period of vector sequence are studied. In the case of maximal length sequence, it is shown that the individual rows are shifted versions of the same binary sequence, and the amount of shifts is calculated.

An expression for the total response in terms of the input sequence, the initial contents of the shift register and the circuit constants is derived. The periods of the output sequence are calculated for cases when the input period is (i) relatively prime to (ii) integral multiple of, and (iii) equal to the autonomous period.

3.1 Circuit Description by State Equation :-

As has been discussed in Chapter 1, LFSR circuits are special class of linear sequential circuits, and such a circuit with single input and single output can be described by the equations :

$$\underset{\sim}{X}(k+1) = \overset{\sim}{\underset{\sim}{A}}\,\underset{\sim}{X}(k) + \underset{\sim}{B}\,U(k) \qquad 3.1\text{-}1$$

$$Y(k) = \underset{\sim}{C}\,\underset{\sim}{X}(k) + D\,U(k) \qquad 3.1\text{-}2$$

where $\underset{\sim}{X}(k)$ is the state vector, $U(k)$ and $Y(k)$ are the input and output respectively, and $\overset{\sim}{\underset{\sim}{A}}$, $\underset{\sim}{B}$, $\underset{\sim}{C}$ and D are matrices of the following form,

$$\overset{\sim}{\underset{\sim}{A}} = \begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_{m-1} & C_m \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \qquad (mxm)$$

$$\underset{\sim}{B} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad (mx1)$$

$$\underset{\sim}{C} = \begin{bmatrix} C_1 & C_2 & C_3 & \cdots & C_{m-1} & C_m \end{bmatrix} \qquad (1xm)$$

and $D = 1 \qquad (1x1)$

C_1, C_2 $\cdots$ C_m are called the tap coefficients. When the LFSR circuit is over the field $GF(2^n)$ with nx1 vector elements the elements of $\overset{\sim}{\underset{\sim}{A}}$, $\underset{\sim}{B}$, $\underset{\sim}{C}$ and D become vectors, and their product is obtained by the method given in Lemma 2.1. Equivalently, elements of $\overset{\sim}{\underset{\sim}{A}}$, $\underset{\sim}{B}$, $\underset{\sim}{C}$ and D can be converted into corresponding nxn matrices, and ordinary multiplication operation may be used. The equations describing the circuit then become

$$\underset{\approx}{X}(k+1) = \underset{\approx}{A}\,\underset{\approx}{X}(k) + \underset{\approx}{B}\,\underset{\sim}{U}(k) \qquad 3.1\text{-}3$$

$$\underline{\underline{Y}}^{(k)} = \underline{\underline{\tilde{C}}}\,\underline{\underline{\tilde{X}}}^{(k)} + \underline{\underline{D}}\,\underline{U}^{(k)} \qquad 3.1\text{-}4$$

where

$$\underline{\underline{\tilde{A}}} = \begin{bmatrix} \underline{\underline{C}}_1 & \underline{\underline{C}}_2 & \underline{\underline{C}}_3 & \cdots & \underline{\underline{C}}_{m-1} & \underline{\underline{C}}_m \\ \underline{\underline{I}} & \underline{\underline{\phi}} & \underline{\underline{\phi}} & \cdots & \underline{\underline{\phi}} & \underline{\underline{\phi}} \\ \vdots & & & & & \\ \underline{\underline{\phi}} & \underline{\underline{\phi}} & \underline{\underline{\phi}} & \cdots & \underline{\underline{I}} & \underline{\underline{\phi}} \end{bmatrix} \qquad 3.1\text{-}5(a)$$

$$\underline{\underline{\tilde{B}}} = \begin{bmatrix} \underline{\underline{I}} \\ \underline{\underline{\phi}} \\ \vdots \\ \underline{\underline{\phi}} \end{bmatrix} \qquad 3.1\text{-}5(b)$$

$$\underline{\underline{\tilde{C}}} = \begin{bmatrix} \underline{\underline{C}}_1 & \underline{\underline{C}}_2 & \underline{\underline{C}}_3 & \cdots & \underline{\underline{C}}_m \end{bmatrix}$$

and $\underline{\underline{D}} = \underline{\underline{I}}$

$\underline{\underline{I}}$ and $\underline{\underline{\phi}}$ are unit and zero elements of $GF(2^n)$ and are unit and null matrices respectively. Here $\underline{\underline{\tilde{X}}}$ is the state vector whose elements are the state variables $\underline{\underline{X}}_1, \underline{\underline{X}}_2, \cdots, \underline{\underline{X}}_m$ and these state variables are elements of $GF(2^n)$ and themselves vectors. $\underline{\underline{\tilde{A}}}$, $\underline{\underline{\tilde{B}}}$, $\underline{\underline{\tilde{C}}}$ and $\underline{\underline{D}}$ are matrices of the form described earlier, but their elements are nxn matrices representing elements of $GF(2^n)$ and therefore are the powers of the companion matrix $\underline{\underline{M}}$. $\underline{U}^{(k)}$ and $\underline{Y}^{(k)}$ denote the input and output sequences of n-tuples respectively.

For the case of $GF(2^n)$ which is considered in this chapter, the polynomial $q(x)$ has coefficients from $GF(2)$ and therefore becomes

$$q(x) = 1 + q_1 x + q_2 x^2 + \cdots + q_{n-1} x^{n-1} + x^n \qquad 3.1\text{-}6$$

and for the companion matrix given by Eq. 2.2-11 $q_o = 1$ and $q_i \in GF(2)$.

The LFSR circuit over $GF(2^n)$ is shown in Fig. 3.1.

Example 3.1 : Find the LFSR circuit whose tap coefficients are

$$\underline{C}_1 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \; ; \; \underline{C}_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \; ; \; \underline{C}_3 = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \; ; \; \underline{C}_4 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$$

and $q(x) = 1+x+x^3$

The companion matrix corresponding to $q(x)$ is

$$\underline{\underline{M}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

The given vectors are converted into corresponding matrices using 2.2-16, giving

$$\underline{\underline{C}}_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \; ; \; \underline{\underline{C}}_2 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} \; ;$$

$$\underline{\underline{C}}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \; ; \; \underline{\underline{C}}_4 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} .$$

The LFSR circuit is of the type shown in Fig. 3.1 with $\underline{\underline{C}}_1$, $\underline{\underline{C}}_2$, $\underline{\underline{C}}_3$, $\underline{\underline{C}}_4$ given above and $m = 4$.

3.2 Response of LFSR Circuits : In this section, we derive an expression for the total response (output sequence) of the circuit shown in Fig. 3.1. The LFSR circuit is described by

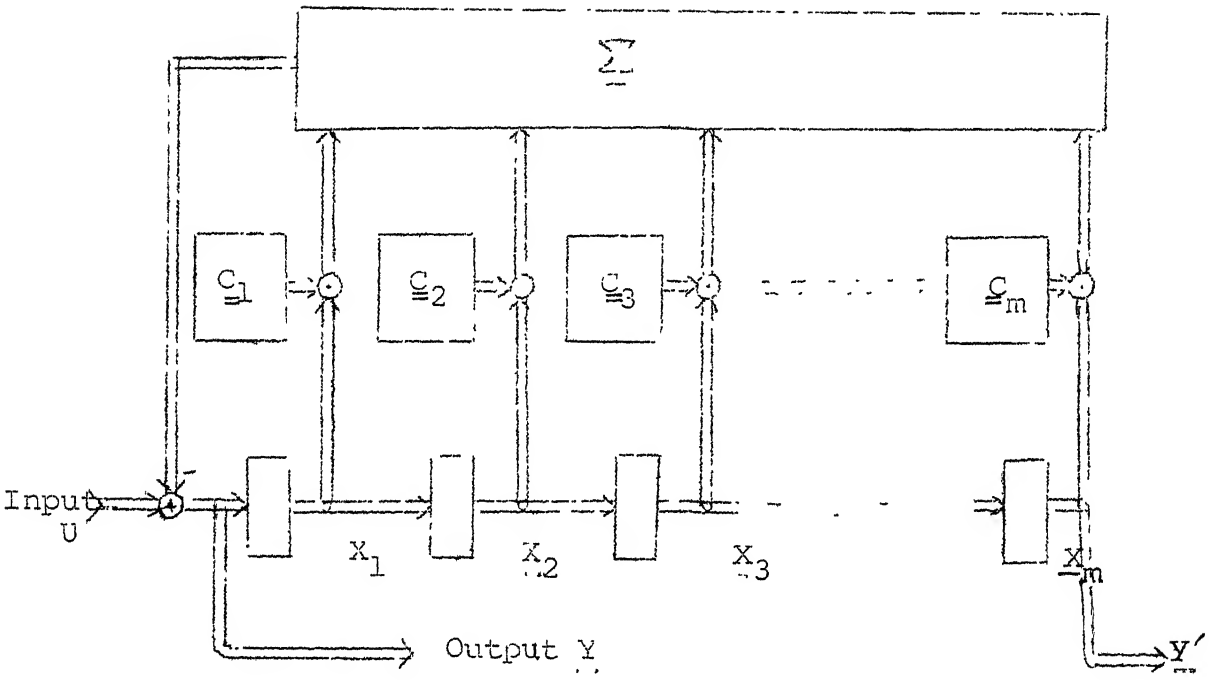


Fig.3.1. LFSR Circuit over GF(2^n)

equations 3.1-3 and 3.1-4 where $\underline{\underline{X}}^2$ is the state vector representing the states $\underline{X}_1\ \underline{X}_2 \cdots \underline{X}_m$ in a mxl vector form, and the individual states are themselves nxl vectors. The states $\underline{X}_1^{(k)}\underline{X}_2^{(k)}\cdots\underline{X}_m^{(k)}$ at instants $k = 1, 2, 3, \cdots$ can be obtained by putting $k = 1, 2, 3, \cdots$ and can be written simultaneously in vector form as $\underline{\underline{X}}^2(1), \underline{\underline{X}}^2(2), \underline{\underline{X}}^2(3)$ ... etc. Therefore from eqn. 3.1-3,

$$\underline{\underline{X}}^2(1) = \underline{\underline{A}}^{22} \cdot \underline{X}^{(0)} + \underline{\underline{B}}^2 \cdot \underline{U}^{(0)}$$

$$\underline{\underline{X}}^2(2) = \underline{\underline{A}}^{22} \cdot \underline{X}^{(1)} + \underline{\underline{B}}^2 \underline{U}^{(1)}$$

$$\cdots$$

$$\underline{\underline{X}}^2(i) = \underline{\underline{A}}^{22} \cdot \underline{X}^{(i-1)} + \underline{\underline{B}}^2 \underline{U}^{(i-1)}$$

Therefore the state sequence $\underline{\underline{X}}^2 = \underline{\underline{X}}^2(0), \underline{\underline{X}}^2(1), \underline{\underline{X}}^2(2) \cdots$ can be written in polynomial form using 2.3-1 as

$$\underline{\underline{X}}^2(d) = \underline{\underline{X}}^2(0) + \underline{\underline{X}}^2(1)d + \underline{\underline{X}}^2(2)d^2 + \underline{\underline{X}}^2(3)\cdot d^3 + \cdots + \cdots + \cdots$$

$$= \underline{\underline{X}}^2(0) + \left[\underline{\underline{A}}^{22}\cdot\underline{\underline{X}}^2(0) + \underline{\underline{B}}^2\ \underline{U}^{(0)}\right] d$$

$$+ \left[\underline{\underline{A}}^{22}\cdot\underline{\underline{X}}^2(1) + \underline{\underline{B}}\ \underline{U}^{(1)}\right] d^2$$

$$+ \left[\underline{\underline{A}}^{22}\cdot\underline{\underline{X}}^2(2) + \underline{\underline{B}}\cdot\underline{U}^{(2)}\right] d^3$$

$$+ \cdots + \cdots + \cdots$$

or $$\underline{\underline{X}}^2(d) = \underline{\underline{X}}^2(0) + \left[\underline{\underline{A}}^{22}\ \underline{\underline{X}}^2(d) + \underline{\underline{B}}^2\ \underline{U}(d)\right] d \qquad 3.2\text{-}1$$

where $\underline{U}(d) = \underline{U}^{(0)} + \underline{U}^{(1)}d + \underline{U}^{(2)}d^2 + \cdots + \cdots$ is the d-transform of the input sequence $\underline{U} = \underline{U}^{(0)}, \underline{U}^{(1)}, \underline{U}^{(2)}, \cdots$ and similarly $\underline{\underline{X}}^2(d)$ is d-transform of state sequence $\underline{\underline{X}}^2$

Eqn. 3.2-1 can be written as

$$\underline{\underline{\underline{X}}}(d) + \underline{\underline{\underline{A}}}\,\underline{\underline{\underline{X}}}(d)\cdot d = \underline{\underline{\underline{X}}}^{(0)} + \underline{\underline{\underline{B}}}\cdot\underline{\underline{U}}(d)\cdot d$$

or $$\underline{\underline{\underline{X}}}(d)\left[\underline{\underline{\underline{I}}} + \underline{\underline{\underline{A}}}\,d\right] = \left[\underline{\underline{\underline{X}}}^{(0)} + \underline{\underline{\underline{B}}}\cdot\underline{\underline{U}}(d)\cdot d\right]$$

or $$\underline{\underline{\underline{X}}}(d) = \left[\underline{\underline{\underline{I}}} + \underline{\underline{\underline{A}}}\,d\right]^{-1}\cdot\left[\underline{\underline{\underline{X}}}^{(0)} + \underline{\underline{\underline{B}}}\cdot\underline{\underline{U}}(d)d\right] \qquad 3.2\text{-}2$$

where $\underline{\underline{\underline{I}}}$ is a unit matrix of size mnxmn such that $\underline{\underline{\underline{I}}}\,\underline{\underline{\underline{X}}}(d) = \underline{\underline{\underline{X}}}(d)$ and it will be shown later that the above inverse exists.

The elements of the output sequence can similarly be obtained by putting k = 0, 1, 2, ... in eqn. 3.1-2 and therefore the d-transform of the output sequence $\underline{Y}$ becomes

$\underline{Y}(d) = \underline{\underline{\underline{C}}}\,\underline{\underline{\underline{X}}}(d) + \underline{\underline{D}}\,\underline{\underline{U}}(d)$ and use of 3.2-2 yields

$$\underline{Y}(d) = \underline{\underline{\underline{C}}}\cdot\left[\underline{\underline{\underline{I}}} + \underline{\underline{\underline{A}}}\,d\right]^{-1}\cdot\left[\underline{\underline{\underline{X}}}^{(0)} + \underline{\underline{\underline{B}}}\cdot\underline{\underline{U}}(d)d\right] + \underline{\underline{D}}\,\underline{\underline{U}}(d) \qquad 3.2\text{-}3$$

This is the expression for the output sequence in terms of the input sequence, initial conditions, and circuit constants which are determined by the matrices $\underline{\underline{\underline{A}}}$ $\underline{\underline{\underline{B}}}$ $\underline{\underline{\underline{C}}}$ and $\underline{\underline{D}}$. Now we shall study various cases for various choices of $\underline{U}(d)$ and $\underline{\underline{\underline{X}}}^{(0)}$.

3.3 Autonomous Response : The autonomous response of a LFSR circuit is defined as the response of the circuit to the input $\underline{0}\ \underline{0}\ \underline{0}\ \ldots$. In other words, the input is absent, and the output sequence depends upon the contents of the delays only.

Mathematically $\underline{U}(d) = \underline{0}$ and eqn. 3.2-3 becomes.

$$\therefore\ \underline{\underline{\underline{Y}}}(d) = \underline{\underline{\underline{C}}}\left[\underline{\underline{\underline{I}}} + \underline{\underline{\underline{A}}}d\right]^{-1}\cdot\underline{\underline{\underline{X}}}^{(0)} \qquad 3.3\text{-}1$$

If $\underline{Y}$ is the autonomous response of a LFSR circuit then we say that the LFSR circuit generates $\underline{Y}$.

3.3-1 Expression for Autonomous Response : The expression for the d-transform of output sequence involves the inverse of the mnxmn matrix $[\underline{\underline{I}}^{22} + \underline{\underline{\tilde{A}}}d]$. We shall derive a simplified expression for $\underline{Y}(d)$ and will show that $\underline{Y}(d)$ can be written as $\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d)$, where $\underline{\underline{C}}(d)$ is a nxn matrix and $\underline{P}(d)$ is a nxl vector of binary polynomials.

Since

$$\underline{\underline{I}}^{22} + \underline{\underline{A}}^{22}d = \begin{bmatrix} \underline{\underline{I}} + \underline{\underline{C}}_1 d & \underline{\underline{C}}_2 d & \cdots & \underline{\underline{C}}_{m-1} & \underline{\underline{C}}_m d \\ \underline{\underline{I}}d & \underline{\underline{I}} & \cdots & \underline{\underline{\varphi}} & \underline{\underline{\varphi}} \\ \underline{\underline{\varphi}} & \underline{\underline{I}}d & \cdots & \underline{\underline{\varphi}} & \underline{\underline{\varphi}} \\ \vdots & & & & \\ \underline{\underline{\varphi}} & \underline{\underline{\varphi}} & \cdots & \underline{\underline{I}}d & \underline{\underline{I}} \end{bmatrix}$$

therefore

$$[\underline{\underline{I}}^{22} + \underline{\underline{A}}^{22}d]^{-1} \begin{bmatrix} \underline{\underline{I}} & \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-1} & \sum_{i=3}^{m} \underline{\underline{C}}_i d^{i-2} & \cdots & \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+2} & \underline{\underline{C}}_m d \\ \underline{\underline{I}}d & \underline{\underline{I}} + \underline{\underline{C}}_1 d & \sum_{i=3}^{m} \underline{\underline{C}}_i d^{i-1} & \cdots & \sum_{m-1}^{m} \underline{\underline{C}}_i d^{i-m+3} & \underline{\underline{C}}_m d^2 \\ \underline{\underline{I}}d^2 & (\underline{\underline{I}} + \underline{\underline{C}}_1 d)d & \underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2 & \cdots & \sum_{m-1}^{m} \underline{\underline{C}}_i d^{i-m+4} & \underline{\underline{C}}_m d^3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \underline{\underline{I}}d^{m-1} & (\underline{\underline{I}} + \underline{\underline{C}}_1 + d)d^{m-2} & (\underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2)d^{m-3} & \cdots & (\underline{\underline{I}} + \sum_{i=1}^{m-2} \underline{\underline{C}}_i d^i)d & \underline{\underline{I}} + \sum_{i=1}^{m-1} \underline{\underline{C}}_i d^i \end{bmatrix}$$

$$\times [\underline{\underline{C}}(d)]^{-1}$$

Where $\underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2 + \cdots + \cdots + \underline{\underline{C}}_m d^m$ 3.3-2

is equal to the determinant of the matrix $[\underline{\underline{I}}+\underline{\underline{A}}d]$ and is defined* as the connection polynomial, or the feedback polynomial of the LFSR circuit.

Multiplication of $\underline{\underline{C}}$ with $[\underline{\underline{I}} + \underline{\underline{A}}d]^{-1}$ yields

$$\underline{\underline{C}}\cdot[\underline{\underline{I}}+\underline{\underline{A}}d]^{-1} = [\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \quad \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-2} \quad \sum_{i=3}^{m} \underline{\underline{C}}_i d^{i-3} \cdots \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+1} \underline{\underline{C}}_m] \times [\underline{\underline{C}}(d)]^{-1} \qquad 3.3\text{-}3$$

Therefore eqn. 3.3-1 becomes

$$\underline{Y}(d) = \underline{\underline{C}}[\underline{\underline{I}} + \underline{\underline{A}}d]^{-1} \underline{X}(0)$$

$$= [\underline{\underline{C}}(d)]^{-1} [\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \quad \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-2} \cdots \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+1} \underline{\underline{C}}_m] \cdot \begin{bmatrix} \underline{X}_1^{(0)} \\ \underline{X}_2^{(0)} \\ \vdots \\ \underline{X}_m^{(0)} \end{bmatrix}$$

$$= [\underline{\underline{C}}(d)]^{-1} \Big[\underline{\underline{C}}_1 \underline{X}_1^{(0)} + \underline{\underline{C}}_2 \underline{X}_2^{(0)} + \underline{\underline{C}}_3 \underline{X}_3^{(0)} + \cdots + \cdots + \underline{\underline{C}}_m \underline{X}_m^{(0)}$$

$$+ (\underline{\underline{C}}_2 \underline{X}_1^{(0)} + \underline{\underline{C}}_3 \underline{X}_2^{(0)} + \cdots + \cdots + \underline{\underline{C}}_m \underline{X}_{m-1}^{(0)}) d$$

$$+ (\underline{\underline{C}}_3 \underline{X}_1^{(0)} + \cdots + \cdots + \underline{\underline{C}}_m \underline{X}_{m-2}) d^2$$

$$+ \cdots$$

$$+ \cdots$$

$$+ \underline{\underline{C}}_m \underline{X}_1^{(0)} \, d^{m-1} \Big]$$

or

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} [\sum_{j=0}^{m-1} \sum_{i=1}^{m-j} \underline{\underline{C}}_{i+j} \cdot \underline{X}_i^{(0)} \cdot d^j] \qquad 3.3\text{-}4$$

---

* $[\underline{\underline{C}}(d)]^{-1}$ is defined in Appendix A.

Therefore the output sequence $\underline{Y}$ is given in terms of its d-transform by

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \underline{P}(d) \qquad 3.3\text{-}5$$

where $$\underline{P}(d) = \sum_{j=0}^{m-1} \sum_{i=1}^{m-j} \underline{\underline{C}}_{i+j} \underline{X}_{i}^{(0)} d^{j} \qquad 3.3\text{-}6$$

and $\underline{\underline{C}}(d)$ is given by 3.3-2.

Sometimes the output Y' is drawn from the last stage. In this case the matrices $\underline{\underline{\tilde{C}}}$ and $\underline{\underline{D}}$ are modified as

$$\underline{\underline{\tilde{C}}} = [\underline{\underline{\varphi}} \; \underline{\underline{\varphi}} \; \cdots \; \underline{\underline{\varphi}} \; \underline{\underline{I}}] \quad \text{and} \quad \underline{\underline{D}} = \underline{\underline{\varphi}}$$

Therefore

$$\underline{Y}'(d) = \underline{\underline{\tilde{C}}} \cdot [\underline{\underline{I}}^{22} + \underline{\underline{A}}^{22} d]^{-1} \cdot \underline{X}^{22}(0)$$

$$= [\underline{\underline{C}}(d)]^{-1} \cdot [\underline{\underline{I}} d^{m-1} (\underline{\underline{I}} + \underline{\underline{C}}_1 d) d^{m-2} (\underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2) d^{m-3} \cdots \underline{\underline{I}} + \sum_{i=1}^{m-1} \underline{\underline{C}}_i d^{i}] \begin{bmatrix} \underline{X}_1^{(0)} \\ \underline{X}_2^{(0)} \\ \vdots \\ \underline{X}_m^{(0)} \end{bmatrix}$$

$$= [\underline{\underline{C}}(d)]^{-1} \cdot [\underline{X}_m^{(0)} + (\underline{\underline{C}}_1 \underline{X}_m^{(0)}) d +$$

$$+ (\underline{\underline{C}}_2 \cdot \underline{X}_m + \underline{\underline{C}}_1 \cdot \underline{X}_{m-1} + \underline{X}_{m-2}) d^2 + \cdots + \cdots + (\sum_{i=1}^{m-1} \underline{\underline{C}}_i \underline{X}_{m-i+1}^{(0)} + \underline{X}_1^{(0)}) d^{m-1}]$$

$$= \underline{\underline{C}}(d)^{-1} \cdot [\sum_{j=0}^{m-1} \sum_{i=0}^{j} \underline{\underline{C}}_{j-i} \underline{X}_{m-i}^{(0)} d^{j}] \, , \; \underline{\underline{C}}_0 = \underline{\underline{I}}$$

or $$\underline{Y}'(d) = [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}'(d) \qquad 3.3\text{-}7$$

where $$\underline{P}'(d) = \sum_{j=0}^{m-1} \sum_{i=0}^{j} \underline{\underline{C}}_{j-i} \underline{X}_{m-i}^{(0)} \cdot d^{j}, \; \underline{\underline{C}}_0 = \underline{\underline{I}} \qquad 3.3\text{-}8$$

Example 3.2 : Find the autonomous response of a 3 stage LFSR circuit over $GF(2^2)$ given

$$\underline{C}_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}; \ \underline{C}_2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}; \ \underline{C}_3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ q(x) = 1+x+x^2;$$

$$\underline{X}_1^{(0)} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}; \ \underline{X}_2^{(0)} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}; \ \underline{X}_3^{(0)} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Here companion matrix corresponding to $q(x)$ is $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

$$\underline{\underline{C}}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}; \ \underline{\underline{C}}_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}; \ \underline{\underline{C}}_3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\underline{P}(d) = \sum_{j=0}^{3-1} \sum_{i=1}^{3-j} \underline{\underline{C}}_{i+j} \underline{X}_i^{(0)} d^j \quad \text{using 3.3-5}$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \end{bmatrix} d + \begin{bmatrix} 0 \\ 1 \end{bmatrix} d^2 = \begin{bmatrix} 0 \\ d^2 \end{bmatrix}$$

$$\underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2 + \underline{\underline{C}}_3 d^3 \quad \text{using 3.3-2}$$

$$= \begin{bmatrix} 1 + d^2+d^3 & d+d^2 \\ d+d^2 & 1+d+d^3 \end{bmatrix}$$

$$\therefore [\underline{\underline{C}}(d)]^{-1} = \begin{bmatrix} 1+d+d^3 & d+d^2 \\ d+d^2 & 1+d^2d^3 \end{bmatrix} \cdot \frac{1}{1+d+d^3+d^5+d^6}$$

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) = \begin{bmatrix} 1+d+d^3 & d+d^2 \\ d+d^2 & 1+d^2+d^3 \end{bmatrix} \begin{bmatrix} 0 \\ d^2 \end{bmatrix} \cdot \frac{1}{1+d+d^3+d^5+d^6}$$

$$= \begin{bmatrix} d^3+d^4 \\ d^2+d^4+d^5 \end{bmatrix} \cdot \frac{1}{1+d+d^3+d^5+d^6}$$

$$= \begin{bmatrix} (d^3+d^4)(1+d+d^2+d^4+d^5+d^6) \\ (d^2+d^4+d^5)(1+d+d^2+d^4+d^5+d^6) \end{bmatrix} \cdot \frac{1}{1+d^{12}}$$

$$= \begin{bmatrix} d^3+d^6+d^7+d^{10} \\ d^2+d^3+d^6+d^{11} \end{bmatrix} \frac{1}{1+d^{12}}$$

Output sequence $\underset{\sim}{Y} = \underset{\sim}{Y}(d) \cdot \delta$

$$= \{^{000100110010}_{001100100001}\} \text{ with period 12}$$

Similarly using 3.3-7, $\underset{\sim}{P}(d) = \begin{bmatrix} d \\ 0 \end{bmatrix}$

and $\underset{\sim}{Y}'(d) = [\underset{\sim}{C}(d)]^{-1} \cdot \underset{\sim}{P}(d) = \begin{bmatrix} d+d^6+d^9+d^{10} \\ d^2+d^5+d^6+d^9 \end{bmatrix} \frac{1}{1+d^{12}}$ using 3.3-8

The sequence drawn from the last stage is

$$\underset{\sim}{Y}' = \underset{\sim}{Y}'(d) \cdot \delta = \{^{010000100110}_{001001100100}\} \text{ with period 12.}$$

And we can verify that $\underset{\sim}{Y}'$ is same as $\underset{\sim}{Y}$ delayed by m = 3 bits.

3.3-2. Properties of Autonomous Response : We have seen that the sequence of binary nxl vectors can be viewed as n binary sequences put row by row, so that the vector formed by taking k^{th} element of these sequences becomes the k^{th} element of the vector sequence for all $k > 0$.

In this section, we show that these row sequences are periodic, and the period of vector sequence is equal to the LCM of the periods of individual rows. Also the vector sequence

can be generated by an equivalent mn stage binary LFSR circuit. This result can be put as the following lemma.

Lemma 3.1 : The vector sequence generated by a m stage LFSR circuit over $GF(2^n)$ can be viewed as n binary sequences put row by row such that,

(i) the row sequences are periodic

(ii) all row sequences can be generated by the same equivalent mn stage LFSR circuit over GF(2)

(iii) the period of vector sequence is equal to the LCM of periods of row sequences.

Proof : Consider a m stage LFSR circuit on $GF(2^n)$ whose connection polynomial $\underline{\underline{C}}(d)$ is given by 3.3-2. Since the coefficients $\underline{\underline{C}}_i$ of $\underline{\underline{C}}(d)$ are nxn binary matrices, we can write

$$\underline{\underline{C}}_i = [c_{kl}^{(i)}] \quad \text{where } l,k = 1,2,\ldots,n,\ i = 1,2,\ldots,m$$

$c_{kl}^{(i)}$ is the kl^{th} element of the i^{th} coefficient of $\underline{\underline{C}}(d)$.

$$\text{Therefore } \underline{\underline{C}}(d) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} + \begin{bmatrix} c_{11}^{(1)} & c_{12}^{(1)} & c_{13}^{(1)} & \cdots & c_{1n}^{(1)} \\ c_{21}^{(1)} & c_{22}^{(1)} & c_{23}^{(1)} & \cdots & c_{2n}^{(1)} \\ \vdots & & & & \\ c_{n1}^{(1)} & c_{n2}^{(1)} & c_{n3}^{(1)} & \cdots & c_{nn}^{(1)} \end{bmatrix} \cdot d$$

$$+ \cdots + \cdots + \cdots + \begin{bmatrix} c_{11}^{(m)} & c_{12}^{(m)} & \cdots & c_{1n}^{(m)} \\ c_{21}^{(m)} & c_{22}^{(m)} & \cdots & c_{2n}^{(m)} \\ \vdots & & & \\ c_{n1}^{(m)} & c_{n2}^{(m)} & \cdots & c_{nn}^{(m)} \end{bmatrix} \cdot d^m$$

$$= \begin{bmatrix} 1+\sum_{i=1}^{m} c_{11}^{(i)} d^i & \sum_{i=1}^{m} c_{12}^{(i)} d^i & \cdots & \sum_{i=1}^{m} c_{1n}^{(i)} d^i \\ \sum_{i=1}^{m} c_{21}^{(i)} d^i & 1+\sum_{i=1}^{m} c_{22}^{(i)} d^i & \cdots & \sum_{i=1}^{m} c_{2n}^{(i)} d^i \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \sum_{i=1}^{m} c_{n1}^{(i)} d^i & \sum_{i=1}^{m} c_{n2}^{(i)} d^i & \cdots & 1+\sum_{i=1}^{m} c_{nn}^{(i)} d^i \end{bmatrix}$$

Therefore $\underline{\underline{C}}(d) = \begin{bmatrix} c_{11}(d) & c_{12}(d) & \cdots & c_{1n}(d) \\ c_{21}(d) & c_{22}(d) & \cdots & c_{2n}(d) \\ \vdots & & \vdots & \\ c_{n1}(d) & c_{n2}(d) & \cdots & c_{nn}(d) \end{bmatrix}$ 3.3-9

where $c_{ij}(d) = \sum_{\ell=1}^{m} c_{ij}^{(\ell)} d^{\ell} \quad i \neq j$

$$c_{ii}(d) = 1+\sum_{\ell=1}^{m} c_{ij}^{(\ell)} d^{\ell} \quad , \quad i,j = 1,2,\cdots,n$$

$$\underline{P}(d) = \begin{bmatrix} p_1(d) \\ p_2(d) \\ \vdots \\ p_n(d) \end{bmatrix}$$

where $p_i(d) = p_o^{(i)} + p_1^{(i)} d + p_2^{(i)} d^2 + \cdots p_{m-1}^{(i)} d^{m-1}$,

$i = 1,2,\cdots,n$

and $p_j^{(i)}$ is the i^{th} row of the coefficient of d^j in the polynomial $\underline{P}(d)$ given by 3.3-6

The inverse of the matrix $\underline{\underline{C}}(d)$ can be obtained using ordinary matrix inversion procedure. Thus

$$[\underline{\underline{c}}(d)]^{-1} = \begin{bmatrix} c'_{11}(d) & c'_{12}(d) \cdots c'_{1n}(d) \\ c'_{21}(d) & c'_{22}(d) \cdots c'_{2n}(d) \\ \vdots & \vdots \quad \ddots \quad \vdots \\ c'_{n1}(d) & c'_{n2}(d) \cdots c'_{nn}(d) \end{bmatrix} \cdot \frac{1}{N(d)} = \underline{\underline{C}}'(d) \cdot \frac{1}{N(d)} \qquad 3.3\text{-}10$$

where $c'_{ij}(d)$ is the cofactor of $c_{ji}(d)$ in 3.3-8 and is a binary polynomial with degree less than $m(n-1)$ and

$N(d) = \text{Det}^{*}[\underline{\underline{c}}(d)]$ and $\deg [N(d)] \leq mn$. (*See Appendix A)

Therefore eqn. 3.3-5 can be written as

$$\underline{Y}(d) = \begin{bmatrix} c'_{11}(d) & c'_{12}(d) & \cdots & c'_{1n}(d) \\ c'_{21}(d) & c'_{22}(d) & \cdots & c'_{2n}(d) \\ \vdots & & & \\ c'_{n1}(d) & c'_{n2}(d) & \cdots & c'_{nn}(d) \end{bmatrix} \cdot \begin{bmatrix} p_1(d) \\ p_2(d) \\ \vdots \\ p_n(d) \end{bmatrix} \cdot \frac{1}{N(d)}$$

$$= \begin{bmatrix} f_1(d) \\ f_2(d) \\ \vdots \\ f_n(d) \end{bmatrix} \cdot \frac{1}{N(d)} \qquad 3.3\text{-}11$$

which can also be written as

$$\underline{Y}(d) = \begin{bmatrix} f_1(d)/N(d) \\ f_2(d)/N(d) \\ \vdots \\ f_n(d)/N(d) \end{bmatrix} = \begin{bmatrix} R_1(d) \\ R_2(d) \\ \vdots \\ R_n(d) \end{bmatrix} \qquad 3.3\text{-}12$$

where $R_i(d) = \dfrac{f_i(d)}{N(d)} = \dfrac{f'_i(d)}{N_i(d)}$, $i = 1, 2, \ldots, n$ 3.3-13

such that $f'_i(d)$ and $N_i(d)$ are relatively prime.

We see that rows of the sequence $\underline{Y}$ are represented by ratio of two binary polynomials and therefore are binary sequence with period equal to exponent of the denominator polynomial. Thus first part of Lemma is proved.

The denominator of each polynomial $R_i(d)$ is the same binary polynomial $N(d)$ with degree mn. Therefore the sequences represented by these polynomials can be generated by a binary LFSR circuit whose connection polynomial is $N(d)$ and therefore it will be a mn stage LFSR circuit. Hence second part is proved.

Equation 3.3-12 can be written with the help of 3.3-13 as

$$\underline{Y}(d) = \begin{bmatrix} R_1(d) \\ R_2(d) \\ \vdots \\ R_n(d) \end{bmatrix} = \begin{bmatrix} f'_1(d)/N_1(d) \\ f'_2(d)/N_2(d) \\ \vdots \\ f'_n(d)/N_n(d) \end{bmatrix}.$$

And since $N_1(d)$, $N_2(d)$ ... $N_n(d)$ are all factors of $N(d)$, therefore

$$N(d) = \text{LCM}\left[N_1(d),\ N_2(d)\ \cdots\ N_n(d)\right]$$

$$\text{Exp}\left\{N(d)\right\} = \text{LCM}\left[\text{Exp}\left\{N_1(d)\right\},\ \text{Exp}\left\{N_2(d)\right\} \cdots\ \text{Exp}\left\{N_n(d)\right\}\right]$$

And since $\text{Exp}\left\{N_i(d)\right\}$ represents the period of R_i, i.e. the period of sequence given by $R_i(d)$, we conclude that

$$\text{Period of } \underline{Y} = \text{LCM}\left[\text{Period of } R_1,\ \text{Period of } R_2, \cdots \right.$$
$$\left. \cdots\ \text{Period of } R_n\right]$$

Thus third part of the Lemma is proved.

3.3-3 Maximal Sequences :

In this section we find the LFSR circuit which can generate maximal sequences and study the properties of maximal sequences, which are already developed for a general sequence in preceeding section. First we give the definition of maximal sequence.

A sequence S of elements from GF(q) is said to be maximal if it is periodic with period q^m-1, m is an integer, and each element of the sequence $S = s_0 s_1 s_2 s_3 \ldots$ can be written as a linear combination of past m elements only, with coefficients from GF(q) i.e.

$$s_j = \sum_{i=1}^{m} s_{j-i} q_i \quad , j = m, m+1, \ldots \text{ and } q_i \in GF(q).$$

Alternately, if S can be generated by a m stage LFSR circuit over GF(q) and has period q^m-1, it is maximal.

For the present case, $q = 2^n$ and therefore the maximal sequences have period $(2^n)^m-1$.

Regarding the properties of maximal sequences, and the circuits which can generate them, we construct the following lemmas.

Lemma 3.2 : The connection polynomial of LFSR circuit which can generate a maximal sequence over $GF(2^n)$ is a primitive polynomial over $GF(2^n)$.

Lemma 3.3 [a] : The rows of a maximal sequence over $GF(2^n)$ are shifted versions of a binary maximal sequence which can be

generated by a mn stage LFSR circuit over GF(2), with N(d) as its connection polynomial.

[b]. The numbers of bits by which the rows of a vector maximal sequence are shifted from the first row are integral multiples of a number β given by

$$\beta = \frac{2^{mn}-1}{2^{n}-1}$$

Lemma 3.4. If $\underline{\underline{A}}(d) = \underline{\underline{I}} + \underline{\underline{A}}_1 d + \underline{\underline{A}}_2 d^2 + \ldots + \underline{\underline{A}}_m d^m$ is a primitive polynomial over $GF(2^n)$ and $\underline{\underline{B}}(d) = \underline{\underline{I}} + \underline{\underline{A}}_1^{1/2} d + \underline{\underline{A}}_2^{1/2} d^2 + \ldots + \underline{\underline{A}}_m^{1/2} d^m$ is another polynomial then $\underline{\underline{B}}(d)$ is also primitive, and the amounts of shifts β_i for the sequence generated by a LFSR circuit with $\underline{\underline{B}}(d)$ as its connection polynomial are double of the amounts of respective shifts β_i for the sequence generated by a LFSR circuit whose connection polynomial is $\underline{\underline{A}}(d)$, and the row sequences in both cases are shifted versions of the same binary sequence.

Proof of Lemma 3.2 :

The d-transform of the autonomous response of a m-stage LFSR circuit over $GF(2^n)$ is given, using Eq. 3.3-11 by

$$\underline{Y}(d) = \underline{\underline{c}}'(d) \cdot \underline{P}(d) \cdot \frac{1}{N(d)}$$

Therefore period of $\underline{Y}$ = Exp. $[N(d)]$

And since $\underline{Y}$ is given to be maximal, its period is $2^{nm}-1$

i.e. $\quad \text{Exp}\,[N(d)] = 2^{nm}-1$

Therefore* $\quad \text{Exp}\,[\underline{\underline{c}}(d)] = 2^{nm}-1$

$$= (2^n)^m - 1$$

*See Appendix B

Since $\underline{c}(d)$ is polynomial of degree m over $GF(2^n)$, and has exponent $(2^n)^m-1$, from the definition of primitive polynomial we conclude that $\underline{c}(d)$ is a primitive polynomial over $GF(2^n)$

Proved

Proof of Lemma 3.3 [a] :

Recalling Eqs. 3.3-11, 3.3-12 and 3.3-13, the i^{th} row of the sequence $\underline{Y}$ is given by

$$R_i(d) = \frac{f_i(d)}{N(d)}, \quad i = 1,2,\ldots,n$$

where $f_i(d)$ is relatively prime to $N(d)$ since $N(d)$ is primitive. Also Exp $[N(d)] = 2^{nm}-1$ = Period of R_i. Therefore R_i is a maximal sequence.

Since all the rows R_i of the sequence $\underline{Y}$ are represented by ratios of two polynomials in d such that they have same denominators, we conclude from the properties of maximal sequences that each row R_i is a shifted version of the same sequence R_1 given by,

$$R_1(d) = \frac{f_1(d)}{N(d)} = \frac{F_1(d)}{1+d^{2^{nm}-1}} \qquad 3.3\text{-}14$$

And $R_1(d)$ can be generated by a LFSR circuit whose connection polynomial is $N(d)$ and therefore number of stages is equal to degree of $N(d)$ which is mn

Proved

Proof of Lemma 3.3 [b] :

Since all rows of the sequence $\underline{Y}$ are shifted versions of the first row R_1, the elements of the row sequences $R_i^{(k)}$ can be

written as

$$R_i^{(k)} = R_1^{(k-\beta_i)}, \quad i = 2, 3, \ldots, n \quad \text{for all } k$$

where β_i is the amount of shift for i^{th} row. Eq. 3.3-12 becomes

$$\underline{Y}^{(k)} = \begin{bmatrix} R_1^{(k)} \\ R_2^{(k)} \\ R_3^{(k)} \\ \vdots \\ R_n^{(k)} \end{bmatrix} = \begin{bmatrix} R_1^{(k)} \\ R_1^{(k-\beta_2)} \\ R_1^{(k-\beta_3)} \\ \vdots \\ R_1^{(k-\beta_n)} \end{bmatrix} \quad \text{for all } k \qquad 3.3\text{-}15$$

In absence of input, Eq. 3.1-3 can be written as

$$\underline{\underline{X}}^{(k+1)} = \underline{\underline{A}}\,\underline{\underline{X}}^{(k)}$$

or

$$\underline{X}_1^{(k+1)} = \underline{\underline{c}}_1 \cdot \underline{X}_1^{(k)} + \underline{\underline{c}}_2 \cdot \underline{X}_2^{(k)} + \ldots + \ldots + \underline{\underline{c}}_m \underline{X}_m^{(k)} \qquad 3.3\text{-}16$$

and

$$\underline{X}_i^{(k+1)} = \underline{X}_{i-1}^{(k)} \qquad i = 2, 3, \ldots, m$$

Therefore

$$\underline{X}_1^{(k+1)} = \underline{\underline{c}}_1 \underline{X}_1^{(k)} + \underline{\underline{c}}_2 \underline{X}_1^{(k-1)} + \underline{\underline{c}}_3 \underline{X}_1^{(k-2)} + \ldots + \ldots + \underline{\underline{c}}_m \underline{X}_1^{(k-m+1)}$$

or

$$\underline{X}_1^{(k+1)} = \sum_{i=1}^{m} \underline{\underline{c}}_i \cdot \underline{X}_1^{(k-i+1)} \qquad 3.3\text{-}17$$

Eq. 3.1-4 gives

$$\underline{Y}^{(k)} = \underline{\underline{C}}\,\underline{\underline{X}}^{(k)}$$

$$= \underline{\underline{c}}_1 \underline{X}_1^{(k)} + \underline{\underline{c}}_2 \underline{X}_2^{(k)} + \ldots + \ldots + \underline{\underline{c}}_m \underline{X}_m^{(k)}$$

$$= \underline{X}_1^{(k+1)} \text{ using 3.3-16.}$$

Therefore Eq. 3.3-17 can be written in terms of $\underline{Y}$ as

$$\underline{Y}(k) = \sum_{i=1}^{m} \underline{\underline{C}}_i \underline{Y}(k-i) \qquad 3.3\text{-}18$$

The tap coefficients $\underline{\underline{C}}_i$'s are matrices corresponding to elements of $GF(2^n)$ and are therefore some power of the companion matrix $\underline{\underline{M}}$. Writing $\underline{\underline{C}}_i = \underline{\underline{M}}^{e_i}$, and using Eq. 2.2-16 and 3.3-15, Eq. 3.3-18 can be written as

$$\underline{Y}(k) = \sum_{i=1}^{m} \underline{\underline{M}}^{e_i} \underline{Y}(k-i)$$

$$= \sum_{i=1}^{m} [\underline{\alpha}^{e_i} \; \underline{\underline{M}}\cdot\underline{\alpha}^{e_i} \; \underline{\underline{M}}^2\cdot\underline{\alpha}^{e_i} \; \cdots \; M^{n-1}\cdot\underline{\alpha}^{e_i}] \cdot \begin{bmatrix} R_1^{(k-i)} \\ R_1^{(k-\beta_2-i)} \\ R_1^{(k-\beta_3-i)} \\ \vdots \\ R_1^{(k-\beta_n-i)} \end{bmatrix}$$

$$= \sum_{i=1}^{m} [R_1^{(k-i)}\underline{\alpha}^{e_i} + R_1^{(k-\beta_2-i)}\underline{\underline{M}}\cdot\underline{\alpha}^{e_i} + R_1^{(k-\beta_3-i)}\underline{\underline{M}}^2\cdot\underline{\alpha}^{e_i} + \cdots + \cdots + \cdots + \cdots +$$

$$+ R_1^{(k-\beta_n-i)}\underline{\underline{M}}^{n-1}\cdot\underline{\alpha}^{e_i}]$$

$$= \sum_{i=1}^{m} [\underline{\underline{I}}\, R_1^{(k-i)} + \underline{\underline{M}}\, R_1^{(k-\beta_2-i)} + \underline{\underline{M}}^2 R_1^{(k-\beta_3-i)} + \cdots + \cdots + \cdots +$$

$$+ \underline{\underline{M}}^{n-1} R_1^{(k-\beta_n-i)}] \cdot \underline{\alpha}^{e_i}$$

Using only first two columns of the matrices $\underline{\underline{I}}$, $\underline{\underline{M}}$, $\underline{\underline{M}}^2$, ... we can write

$$\underline{\underline{I}}\, R_1^{(k-i)} = \begin{bmatrix} 1 & 0 & \cdots & \cdots \\ 0 & 1 & \cdots & \cdots \\ 0 & 0 & \cdots & \cdots \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & \cdots \end{bmatrix} R_1^{(k-i)} = \begin{bmatrix} R_1^{(k-i)} & 0 & \cdots & \cdots \\ 0 & R_1^{(k-i)} & \cdots & \cdots \\ 0 & 0 & & \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & \cdots \end{bmatrix}$$

$$\underline{\underline{M}} R_1^{(k-\beta_2-i)} = \begin{bmatrix} 0 & 0 & \cdots & \cdots \\ 1 & 0 & \cdots & \cdots \\ 0 & 1 & \cdots & \cdots \\ \vdots & \vdots & & \\ 0 & 0 & \cdots & \cdots \end{bmatrix} R_1^{(k-\beta_2-i)} = \begin{bmatrix} 0 & 0 & \cdots \\ R_1^{(k-\beta_2-i)} & 0 & \cdots \\ 0 & R_1^{(k-\beta_2-i)} & \cdots \\ \vdots & \vdots & \\ 0 & 0 & \cdots \end{bmatrix}$$

Similarly we can write $\underline{\underline{M}}^2 R_1^{(k-\beta_3-i)}$, $\underline{\underline{M}}^3 R_1^{(k-\beta_4-i)}$ ... $\underline{\underline{M}}^{n-2} R_1^{(k-\beta_{n-1}-i)}$

and finally

$$\underline{\underline{M}}^{n-1} R_1^{(k-\beta_n-i)} = \begin{bmatrix} 0 & 1 & \cdots \\ 0 & q_1 & \cdots \\ \vdots & \vdots & \\ 1 & q_{n-1} & \cdots \end{bmatrix} R_1^{(k-\beta_n-i)} = \begin{bmatrix} 0 & R_1^{(k-\beta_n-i)} & \cdots \\ 0 & q_1 R_1^{(k-\beta_n-i)} & \cdots \\ 0 & q_2 R_1^{(k-\beta_n-i)} & \cdots \\ \vdots & \vdots & \\ R_1^{(k-\beta_n-i)} & q_{n-1} R_1^{(k-\beta_n-i)} & \cdots \end{bmatrix}$$

Therefore $\underline{Y}^{(k)}$ can be written as,

$$\underline{Y}^{(k)} = \sum_{i=1}^{m} \begin{bmatrix} R_1^{(k-1)} & R_1^{(k-\beta_n-i)} & \cdots & \cdots \\ R_1^{(k-\beta_2-i)} & R_1^{(k-i)} + q_1 R_1^{(k-\beta_n-i)} & \cdots & \cdots \\ R_1^{(k-\beta_3-i)} & R_1^{(k-\beta_2-i)} + q_2 R_1^{(k-\beta_n-i)} & \cdots & \cdots \\ \vdots & \vdots & & \\ R_1^{(k-\beta_n-i)} & R_1^{(k-\beta_{n-1}-i)} + q_{n-1} R_1^{(k-\beta_n-i)} & \cdots & \cdots \end{bmatrix} \cdot \underline{\alpha}^{e_i}$$

Using Eq. 3.3-15, the above vector equation can be splitted into n rows giving,

$$R_1^{(k)} = \sum_{i=1}^{m} [\, R_1^{(k-i)} \quad R_1^{(k-\beta_n-i)} \quad \ldots \quad \ldots \,]\, \underline{\alpha}^{e_i}$$

$$R_1^{(k-\beta_i)} = \sum_{i=1}^{m} [\, R_1^{(k-\beta_2-i)} \quad R_1^{(k-i)} + q_1 R_1^{(k-\beta_n-i)} \ldots \quad \ldots \,]\, \alpha^{e_i}$$

$$R_1^{(k-\beta_j)} = \sum_{i=1}^{m} [\, R_1^{(k-\beta_j-i)} \quad R_1^{(k-\beta_{j-1}-i)} + q_{j-1} R_1^{(k-\beta_n-i)}]\, \alpha^{e_i}, \quad j=3,4,\ldots n$$

The above n equations are representing k^{th} element of the row sequences of $\underline{Y}$ for all values of k. Therefore replacing k by $k+\beta_j$ in above equations, we get,

$$R_1^{(k)} = \sum_{i=1}^{m} [R_1^{(k-i)} \quad R_1^{(k-\beta_n-i)} \quad \ldots \quad \ldots]\underline{\alpha}^{e_i} \text{ [unchanged]}$$

$$R_1^{(k)} = \sum_{i=1}^{m} [R_1^{(k-i)} \quad R_1^{(k+\beta_2-i)} + q_1 R_1^{(k+\beta_2-\beta_n-i)} \quad \ldots]\underline{\alpha}^{e_i}$$

$$R_1^{(k)} = \sum_{i=1}^{m} [R^{(k-i)} \quad R^{(k+\beta_j-\beta_{j-1}-i)} + q_{j-1} R_1^{(k+\beta_j-\beta_n-i)} \ldots]\, \underline{\alpha}^{e_i} \quad j=3,4,\ldots r$$

3.3-19

The above equations are representing the elements of the same sequence R_1. Since we have not put any constraint upon $\underline{\alpha}^{i}$'s, these equations are valid for all $\underline{\alpha}^{i}$ and therefore respective columns of all of the equations 3.3-19 must be equal independently. We see that first columns are the same. Equating second columns, we get

$$R_1^{(k-\beta_n-i)} = R_1^{(k+\beta_2-i)} + q_1 R_1^{(k+\beta_2-\beta_n-i)} \qquad 3.3\text{-}20(1)$$

$$= R_1^{(k+\beta_3-\beta_2-i)} + q_2 R_1^{(k+\beta_3-\beta_n-i)} \qquad 3.3\text{-}20(2)$$

$$= \quad + \ldots$$

$$= \ldots$$

$$= R_1^{(k+\beta_{n-1}-\beta_{n-2}-i)} + q_{n-2} R_1^{(k+\beta_{n-1}-\beta_n-i)} \qquad 3.3\text{-}20(n-2)$$

$$= R_1^{(k+\beta_n-\beta_{n-1}-i)} + q_{n-1} R_1^{(k-i)} \qquad 3.3\text{-}20(n-1)$$

Eq. 3.3-20(1) gives

$$R_1^{(k-\beta_2)} = R_1^{(k+\beta_n)} + q_1 R_1^{(k)} \qquad 3.3\text{-}21(1)$$

Eq. 3.3-20(2) gives

$$R_1^{(k-\beta_3)} = R_1^{(k+\beta_n-\beta_2)} + q_2 R^{(k)}$$

which, with the help of 3.3-21(1), becomes,

$$R_1^{(k-\beta_3)} = (R_1^{(k+\beta_n+\beta_n)} + q_1 R_1^{(k+\beta_n)}) + q_2 R_1^{(k)}$$

$$\text{or } R_1^{(k-\beta_3)} = R_1^{(k+2\beta_n)} + q_1 R_1^{(k+\beta_n)} + q_2 R_1^{(k)} \qquad 3.3\text{-}21(2)$$

Eq. 3.3-20(3) gives

$$R_1^{(k-\beta_4)} = R_1^{(k+\beta_n-\beta_3)} + q_3 R_1^{(k)}$$

which, with the help of 3.3-21(2) becomes

$$R_1^{(k-\beta_4)} = (R_1^{(k+2\beta_n+\beta_n)} + q_1 R_1^{(k+\beta_n+\beta_n)} + q_2 R_1^{(k+\beta_n)}) + q_3 R_1^{(k)}$$

$$\text{or } R_1^{(k-\beta_4)} = R_1^{(k+3\beta_n)} + q_1 R_1^{(k+2\beta_n)} + q_2 R_1^{(k+\beta_n)} + q_3 R_1^{(k)} \qquad 3.3\text{-}21(3)$$

In a similar manner, we proceed to calculate $R_1^{(k-\beta_j)}$, $j=5,6,7\ldots n$ and end up with

$$R_1^{(k-\beta_n)} = R_1^{(k+(n-1)\beta_n)} + q_1 R_1^{(k+(n-2)\beta_n)} + \ldots + \ldots + q_{n-2} R_1^{(k+\beta_n)} + q_{n-1} R_1^{(k)}$$

$$\text{or } R_1^{(k)} = R_1^{(k-n\beta_n)} + q_{n-1} R_1^{(k-(n-1)\beta_n)} + q_{n-2} R_1^{(k-(n-2)\beta_n)} + \ldots + \ldots + q_2 R_1^{(k-2\beta_n)} + q_1 R_1^{(k-\beta_n)}$$

The sequence R_1, whose elements are given by the above equation, can be written in terms of a polynomial in d [see sec. 2.3] as,

$$R_1(d) = R_1(d)\, d^{n\beta_n} + q_{n-1} R_1(d) d^{(n-1)\beta_n} + \ldots + \ldots + q_2 R_1(d) d^{2\beta_n} + q_1 R_1(d) d^{\beta_n}$$

$$= [q_1 d^{\beta_n} + q_2 d^{2\beta_n} + \ldots + \ldots + q_{n-1} d^{(n-1)\beta_n} + d^{n\beta_n}] R_1(d)$$

$$\text{or } R_1(d) = \frac{h(d)}{1 + q_1 d^{\beta_n} + q_2 d^{2\beta_n} + \ldots + \ldots + q_{n-1} d^{(n-1)\beta_n} + d^{n\beta_n}} \qquad 3.3\text{-}22$$

or $$R_1(d) = \frac{h(d)}{q(d^{\beta_n})}. \qquad 3.3\text{-}23$$

where h(d) is some binary polynomial in d with degree less than $n\beta_n$ and $q(d^{\beta_n})$ is defined by replacing x by d^{β_n} in Eq. 3.1-6.

Since q(d) is a primitive polynomial of degree n, we have

$$\text{Exp}\,[q(d)] = 2^n-1$$

therefore* $$\text{Exp}\,[q(d^{\beta_n})] = (2^n-1)\beta_n$$

Eq. 3.3-23 can be written as

$$R_1(d) = \frac{h(d)}{q(d^{\beta_n})} = \frac{h'(d)}{1 + d^{(2^n-1)\beta_n}} \qquad 3.3.24$$

From Eq. 3.3-14 we know that period of R_1 is $2^{nm}-1$. Therefore the period $(2^n-1)\beta_n$ given by 3.2-24 must be an integral multiple of $2^{nm}-1$ i.e.

$$\beta_n(2^n-1) = K.\ (2^{nm}-1)$$

or $$\beta_n = K \cdot \frac{2^{nm}-1}{2^n-1} \qquad K = 1, 2, \ldots, 2^n-1$$

From Eq. 3.3-20, all β_j, $j = 2, 3, \ldots, n-1$ can be calculated in terms of β_n. We conclude that the amounts of shifts $\beta_1, \beta_2, \ldots, \beta_n$ are integral multiple of the number β given by

$$\beta = \frac{2^{nm}-1}{2^n-1} \qquad 3.3\text{-}25$$

Proved

*See Appendix C for proof.

Example 3.3 : Find the amounts of shifts of the rows of the sequence generated by the primitive polynomial $\underline{1}+\underline{\alpha}d+\underline{\alpha}d^2$ where $\underline{\alpha} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is element of $GF(2^3)$ and $q(x) = 1+x+x^3$. Verify that they are integral multiples of β given by 3.3-25.

$$\text{Here } \underline{\underline{M}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & q_1 \\ 0 & 1 & q_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \underline{\underline{\alpha}} = [\underline{\alpha} \;\; \underline{\underline{M}}\cdot\underline{\alpha} \;\; \underline{\underline{M}}^2\underline{\alpha}] = \underline{\underline{M}}$$

$$\therefore \quad \underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{M}}d + \underline{\underline{M}}\,d^2 = \begin{bmatrix} 1 & 0 & d+d^2 \\ d+d^2 & 1 & d+d^2 \\ 0 & d+d^2 & 1 \end{bmatrix}$$

$$[\underline{\underline{C}}(d)]^{-1} = \begin{bmatrix} 1+d^2+d^4 & d^2+d^4 & d+d^2 \\ d+d^2 & \cdot & d+d^4 \\ d^2+d^4 & d+d^2 & 1 \end{bmatrix} \cdot \frac{1}{1+d^2+d^3+d^5+d^6}$$

We see that $N(d) = 1+d^2+d^3+d^5+d^6$ is a primitive polynomial and therefore $\underline{1} + \underline{\alpha}d + \underline{\alpha}d^2$ is also

$$\therefore \quad \underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1}\cdot\underline{P}(d) = \begin{bmatrix} 1+d^2+d^4 & d^2+d^4 & d+d^2 \\ d+d^2 & 1 & d+d^4 \\ d^2+d^4 & d+d^2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \frac{1}{1+d^2+d^3+d^5+d^6}$$

assuming initial contents such that $\underline{P}(d) = \underline{1}$.

$$\text{or} \qquad \underline{Y}(d) = \begin{bmatrix} 1+d^2+d^4 \\ d+d^2 \\ d^2+d^4 \end{bmatrix} \cdot \frac{1}{1+d^2+d^3+d^5+d^6}$$

which gives

$$\underline{Y} = \underline{Y}(d) \cdot \delta = \begin{cases} 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0 \cdots \\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 0 \cdots \\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0 \cdots \end{cases}$$

Here we observe that $\beta_2 = 4$ and $\beta_3 = 54$.

From Eq. 3.3-25 $\beta = \dfrac{2^{mn}-1}{2^n-1} = \dfrac{2^{3\cdot 2}-1}{2^3-1} = \dfrac{63}{7} = 9$

and therefore β_2 and β_3 are integral multiples of β.

Proof of Lemma 3.4

First we define the square roots of the elements of $GF(2^n)$. Since elements of $GF(2^n)$ in matrix form are powers of the companion matrix $\underline{\underline{M}}$, we may write

$$\underline{\underline{A}}_i = \underline{\underline{M}}^{e_i} \qquad \text{where } e_i \text{ is some integer.}$$

Then we define

$$\underline{\underline{A}}_i^{1/2} = \underline{\underline{M}}^{e_i/2} \qquad e_i = \text{even}$$

$$= \underline{\underline{M}}^{\frac{e_i+2^n-1}{2}} \qquad e_i = \text{odd.}$$

Thus square roots of elements of $GF(2^n)$ are also elements of $GF(2^n)$.

Using 3.3-10, the autonomous response $\underline{S}_a$ of a LFSR circuit whose connection polynomial is $\underline{\underline{A}}(d)$ is given by

$$\underline{S}_a = [\underline{\underline{A}}'(d)] \cdot \underline{P}_1(d) \cdot \frac{1}{N(d)}$$

$$= \begin{bmatrix} A'_{11}(d) & A'_{12}(d) & \cdots & A'_{1n}(d) \\ A'_{21}(d) & A'_{21}(d) & \cdots & A'_{2n}(d) \\ \vdots & \vdots & & \vdots \\ A'_{n1}(d) & A'_{n2}(d) & & A'_{nn}(d) \end{bmatrix} \cdot \underline{P}_1(d) \cdot \frac{1}{N(d)} \qquad -3.3\text{-}26$$

where $\underline{P}_1(d)$ is the polynomial corresponding to initial contents. Now the second polynomial $\underline{\underline{B}}(d)$ obtained by taking square roots of coefficients of $\underline{\underline{A}}(d)$ can be written as

$$\underline{\underline{B}}(d) = \underline{\underline{I}} + \underline{\underline{A}}_1^{1/2} d + \underline{\underline{A}}_2^{1/2} d^2 + \cdots + \underline{\underline{A}}_m^{1/2} d^m$$

or
$$[\underline{\underline{B}}(d)]^2 = [\underline{\underline{I}} + \underline{\underline{A}}_1^{1/2} d + \underline{\underline{A}}_2^{1/2} d^2 + \cdots + \underline{\underline{A}}_m^{1/2} d^m]^2$$

$$= [\underline{\underline{I}}]^2 + [\underline{\underline{A}}_1^{1/2} d]^2 + [\underline{\underline{A}}_2^{1/2} d^2]^2 + \cdots + [\underline{\underline{A}}_m^{1/2} d^m]^2$$

$$= \underline{\underline{I}} + \underline{\underline{A}}_1 d^2 + \underline{\underline{A}}_2 d^4 + \cdots + \underline{\underline{A}}_m d^{2m}$$

$$= \underline{\underline{A}}(d^2)$$

Therefore $\underline{\underline{B}}(d) = [\underline{\underline{A}}(d^2)]^{1/2}$

and the sequence generated by the LFSR circuit whose connection polynomial is $\underline{\underline{B}}(d)$ is given by

$$\underline{S}_b(d) = [\underline{\underline{B}}(d)]^{-1} \cdot \underline{P}_2(d)$$

$$= [\underline{\underline{A}}(d^2)]^{-1/2} \cdot \underline{P}_2(d)$$

$$= [\underline{\underline{A}}(d^2)]^{-1} \cdot [\underline{\underline{A}}(d^2)]^{1/2} \cdot \underline{P}_2(d),$$

$$= \begin{bmatrix} A'_{11}(d^2) & A'_{12}(d^2) & \cdots & A'_{1n}(d^2) \\ A'_{21}(d^2) & A'_{22}(d^2) & \cdots & A'_{2n}(d^2) \\ \vdots & \vdots & & \vdots \\ A'_{n1}(d^2) & A'_{n2}(d^2) & \cdots & A'_{nn}(d^2) \end{bmatrix} \cdot \underline{P}'_2(d) \cdot \frac{1}{N(d)} \qquad 3.3\text{-}27$$

where

$\underline{P}'_2(d) = [\underline{\underline{A}}(d^2)]^{1/2} \cdot \underline{P}_2(d)/N(d)$ is a polynomial in d.

Since $\det [\underline{\underline{B}}(d)] = \det [\underline{\underline{A}}(d^2)]^{1/2} = [N(d^2)]^{1/2} = N(d)$, we conclude that the denominator of Eq. 3.3-27 is N(d) only i.e. $\underline{P}_2'(d)$ is a polynomial with denominator 1. Thus rows of $\underline{S}_a$ and $\underline{S}_b$ are shifted version of same sequence since the denominators in both cases are N(d). Since the effect of the initial contents is to introduce a shift in the vector sequence, and the sequence length and amounts of shifts of individual rows are independent of $\underline{P}(d)$, we can choose $\underline{P}_1(d)$ and $\underline{P}_2(d)$ different such that

$$\underline{P}_1(d) = \underline{P}_2'(d).$$

Therefore Eqs. 3.3-26 and 3.3-27 can be written as

$$\underline{S}_a(d) = \begin{bmatrix} f_1(d) \\ f_2(d) \\ \vdots \\ f_n(d) \end{bmatrix} \cdot \frac{1}{N(d)} \quad ; \quad \underline{S}_b(d) = \begin{bmatrix} f_1(d^2) \\ f_2(d^2) \\ \vdots \\ f_n(d^2) \end{bmatrix} \cdot \frac{1}{N(d)} .$$

If $\underline{S}_a$ is written as

$$\underline{S}_a^{(k)} = \begin{bmatrix} R_1^{(k)} \\ R_1^{(k-\beta_2)} \\ R_1^{(k-\beta_3)} \\ \vdots \\ R_1^{(k-\beta_n)} \end{bmatrix}$$

then since numerators of polynomials representing rows of $\underline{S}_b$ are squares of the numerators of polynomials representing rows of $\underline{S}_a$, we can write,

$$\underline{S}_b^{(k)} = \begin{bmatrix} R_1^{(k)} \\ R_1^{(k-2\beta_2)} \\ R_1^{(k-2\beta_3)} \\ \vdots \\ R_1^{(k-2\beta_n)} \end{bmatrix}$$

Thus the amounts of shifts are doubled.

The Equation 3.3-24 for this case becomes $R_b(d) = \frac{h_b'(d)}{1+d^{2\beta_n(2^n-1)}}$, where R_b is the row of $\underline{S}_b$.

Similarly, we can keep on taking square roots of coefficients and find the corresponding sequences generated by $\underline{\underline{I}} + \sum_{i=1}^{m} \underline{\underline{A}}_i^{1/2^j} d^i$, $j = 1,2,\ldots,n-1$. If β_i's are the amounts of shifts for $\underline{\underline{A}}(d)$ and $(2^n-1)\beta_n$ is the exponent of the denominator of the polynomial representing the row of the sequence $\underline{S}_a$ then for the other cases we get the following results :

Coefficients	Shifts	exponents
$\underline{\underline{A}}_i$	β_i	$\beta_n(2^n-1)$
$\underline{\underline{A}}_i^{1/2}$	$2\beta_i$	$2\beta_n(2^n-1)$
$A_i^{1/4}$	$4\beta_i$	$4\beta_n(2^n-1)$
...	...	...
...	...	...
...	...	...
$\underline{\underline{A}}^{1/2^n} = \underline{\underline{A}}_i$	$2^n\beta_i=\beta_i$	$\beta_n(2^n-1)$

And since periods of rows are $2^{nm}-1$ only, these exponents must be integral multiples of $2^{nm}-1$ i.e.,

$$2^{j'}\,\beta_n(2^n-1) = K\cdot(2^{nm}-1), \quad j' = 0,1,2,\ldots,n-1, K = \text{integer}.$$

Which is satisfied for $K = 2^{n-1}$ only.

$$\therefore\ \beta_n(2^n-1) = \frac{2^{n-1}}{2^{j'}}(2^{nm}-1) \quad j' = 0,1,2,\ldots,n-1$$

$$\text{or}\quad \beta_n = \frac{2^{mm}-1}{2^n-1}\cdot 2^j \qquad j = 0,1,2,\ldots,n-1 \qquad 3.3\text{-}28$$

Example 3.4. Consider the primitive polynomial $\underline{\underline{A}}(d) = \underline{\underline{I}} + \underline{\underline{M}}d$ where $\underline{\underline{M}}$ is the companion matrix and $q(x) = 1+x+x^4$. Find the shifts β_j for the sequences generated by $\underline{\underline{I}} + \underline{\underline{M}}^{2^{-j}}d$, $j = 0,1,2,3,\ldots$.

Since $\underline{S}_a = [\underline{\underline{I}} + \underline{\underline{M}}d]^{-1}\cdot \underline{P}(d)\,\delta$

$$= \begin{Bmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1 \end{Bmatrix}.$$ with period 15

we have $\beta_2 = 12$

$\beta_3 = 13$

$\beta_4 = 14$

Therefore for $j = 1$, the sequence $\underline{S}_b$ generated by $\underline{\underline{I}} + \underline{\underline{M}}^{1/2}d$ must have

$\beta_2 = 24 = 24-15 = 9$

$\beta_3 = 26 = 26-15 = 11$

$\beta_4 = 28 = 28-15 = 13$

$$\therefore \quad \underline{S}_b = \begin{Bmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0 \\ 1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0 \end{Bmatrix}$$ with period 15

For j = 2, the sequence $\underline{S}_c$ generated by $\underline{\underline{I}} + \underline{\underline{M}}^{1/4}d$ has

$$\beta_2 = 9 \cdot 2 = 18 = 3$$

$$\beta_3 = 11 \cdot 2 = 22 = 7$$

$$\beta_4 = 13 \cdot 2 = 26 = 11$$

$$\therefore \quad \underline{S}_c \quad \begin{Bmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1 \\ 1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0 \end{Bmatrix}$$ with period 15

For j = 3, the sequence $\underline{S}_d$ generated by $\underline{\underline{I}} + \underline{\underline{M}}^{1/8}d$ has

$$\beta_2 = 3 \cdot 2 = 6$$

$$\beta_3 = 7 \cdot 2 = 14$$

$$\beta_4 = 11 \cdot 2 = 22 = 7$$

$$\therefore \quad \underline{S}_d = \begin{Bmatrix} 1\,0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1 \\ 0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,1\,1\,1 \\ 1\,0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,1\,0\,0\,1 \end{Bmatrix}$$ with period 15.

3.4 Total Response : In this section, the response of the LFSR circuit over $GF(2^n)$ to periodic input sequence over $GF(2^n)$ is studied. The expression for the d-transform of output sequence is derived and the output period is determined when the input period and the autonomous period are (i) relatively prime (ii) integral multiples and (iii) equal. Since the

expressions giving the period of output sequence are similar to those obtained in the case of sequences over GF(2), for which periods are already known [10], the results available for binary case are directly used here, without going into their derivation.

The expression for the response of LFSR circuit is given by 3.2-3. With the use of 3.3-3, it can be written as

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \left[\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \quad \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-2} \quad \sum_{i=3}^{m} \underline{\underline{C}}_i d^{i-3} \cdots \right.$$

$$\left. \cdots \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+1} \quad \underline{\underline{C}}_m d^{i-m+1} \quad \underline{\underline{C}}_m \right] \left[\underline{\tilde{X}}^{(0)} + \underline{\underline{\tilde{B}}} d\underline{U}(d) \right] + \underline{\underline{D}}\, \underline{U}(d)$$

$$= [\underline{\underline{C}}(d)]^{-1} \cdot \left[\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \quad \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-2} \cdots \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+1} \underline{\underline{C}}_m \right] \cdot \underline{\tilde{X}}^{(0)}$$

$$+ [\underline{\underline{C}}(d)]^{-1} \cdot \left[\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \quad \sum_{i=2}^{m} \underline{\underline{C}}_i d^{i-2} \cdots \right.$$

$$\left. \cdots \sum_{i=m-1}^{m} \underline{\underline{C}}_i d^{i-m+1} \quad \underline{\underline{C}}_m \right] \cdot \begin{bmatrix} \underline{\underline{I}} \\ \underline{\underline{\varphi}} \\ \underline{\underline{\varphi}} \\ \vdots \\ \underline{\underline{\varphi}} \end{bmatrix} \cdot d\underline{U}(d) + \underline{\underline{I}}\, \underline{U}(d)$$

$$= [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) + [\underline{\underline{C}}(d)]^{-1} \cdot \left[\sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \right] \cdot d\underline{U}(d) + \underline{\underline{I}}\, \underline{U}(d)$$

using 3.3-6

$$= [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) + [\underline{\underline{C}}(d)]^{-1} \cdot \left\{ \sum_{i=1}^{m} \underline{\underline{C}}_i d^{i-1} \cdot d\, \underline{U}(d) + \underline{\underline{I}}\, \underline{\underline{C}}(d)\, \underline{U}(d) \right\}$$

$$= [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) + [\underline{\underline{C}}(d)]^{-1} \cdot \{ \sum_{i=1}^{m} \underline{\underline{C}}_i d^i \, \underline{U}(d) + (\underline{\underline{I}} + \sum_{i=1}^{m} \underline{\underline{C}}_i d^i) \underline{U}(d) \}$$

using 3.3-2

$$= [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) + [\underline{\underline{C}}(d)]^{-1} \cdot \{ \underline{\underline{I}} \, \underline{U}(d) \}$$

or

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot [\underline{P}(d) + \underline{U}(d)] \qquad 3.4\text{-}1$$

If the input sequence $\underline{U} = \underline{u}_0 \underline{u}_1 \underline{u}_2 \underline{u}_3 \ldots$ is a periodic sequence of vectors with period b, then its d-transform can be written as

$$\underline{U}(d) = \frac{\underline{u}_0 + \underline{u}_1 d + \underline{u}_2 d^2 + \ldots + \ldots + \underline{u}_{b-1} d^{b-1}}{1+d^b} = \frac{\underline{v}(d)}{1+d^b} \qquad 3.4\text{-}2$$

And since $[\underline{\underline{C}}(d)]^{-1} = [\underline{\underline{C}}'(d)] \cdot \frac{1}{N(d)} = [\underline{\underline{C}}''(d)] \cdot \frac{1}{1+d^a}$

where $a = \text{Exp}\,[N(d)] = \text{Exp}\,[\underline{\underline{C}}(d)]$, we can write Eq. 3.4-1 as

$$\underline{Y}(d) = [\underline{\underline{C}}''(d)] \left[\frac{\underline{P}(d)}{1+d^a} + \frac{\underline{v}(d)}{(1+d^b)(1+d^a)} \right] \qquad 3.4\text{-}3$$

We observe that the expression for the response of LFSR circuit to periodic input for $GF(2^n)$ has binary polynomials in the denominator. Since the periods of sequences depend upon the denominators of the polynomials representing them, we conclude that period of $\underline{Y}$ can be calculated in the same manner as it is calculated for the case of sequences over GF(2). Since these results are already known, we don't go into details and write the results directly.

Case I : Input period 'b' is relatively prime to autonomous period 'a' :

i.e. $b \neq r \cdot a$, $r = 1, 2, 3, \ldots$.

In this case $\dfrac{\underline{V}(d)}{(1+d^b)(1+d^a)}$ can be expanded into partial fractions, and the expression for $\underline{Y}(d)$ becomes

$$\underline{Y}(d) = [\underline{\underline{C}}''(d)] \left[\frac{\underline{V}'(d)}{1+d^b} + \frac{\underline{A}(d) + \underline{P}(d)}{1+d^a}\right]$$

When $\underline{P}(d) = \underline{A}(d)$, second terms from above expression vanishes. That is, for one particular initial state corresponding to $\underline{P}(d) = \underline{A}(d)$, the output period is equal to the input period. This state is called the critical state.

For other initial states

Output period = LCM(a,b) = a.b

Case II : Input period is an integral multiple of autonomous period.

$b = a \cdot r$, $r = 2, 3, \ldots$.

In this case output period is an integral multiple of the autonomous period, but not necessarily equal to b.

Output period = $a \cdot r'$, $r' = 1, 2, 3, \ldots$.

Case III : Input period is equal to autonomous period. i.e. b = a. In this case, if initial contents are zero then $\underline{P}(d) = 0$ and

$$\underline{Y}(d) = [\underline{\underline{C}}''' d)] \frac{\underline{V}(d)}{(1+d^a)(1+d^a)} .$$

If $[\underline{C}''(d)]\,\underline{v}(d)$ has a factor $1+d^a$ then output period will be a. Otherwise output period will be 2a.

If the initial states are nonzero then the output period will depend upon the particular initial state and cannot be obtained in terms of a. Details are given in reference [10].

Example 3.5 : The connection polynomial of a LFSR circuit over $GF(2^2)$ is $\underline{C}(d) = \underline{1}+\underline{\alpha}x + \underline{1}x^2$ where $\underline{\alpha}$ is the primitive element $\begin{bmatrix}0\\1\end{bmatrix}$ of $GF(2^2)$ and $q(x) = 1+x+x^2$. Find the period of the output sequence when it is fed in by the sequence $\underline{U} = \underline{1}\ \underline{\alpha}\ \underline{0}\ \underline{0}\ \underline{\alpha}\ \underline{\alpha}^2\ \underline{0}\ \underline{0}\ \underline{\alpha}^2\ \underline{1}\ \underline{0}\ \underline{0}\ \cdots$ with period 12 and initial conditions are

(i) $\underline{X}_1^{(0)} = \underline{1}$; $\underline{X}_2^{(0)} = \underline{0}$

(ii) $\underline{X}_1^{(0)} = \underline{\alpha}$; $\underline{X}_2^{(0)} = \underline{\alpha}^2$.

The companion matrix corresponding to $\underline{\alpha}$ is

$$\underline{\underline{M}} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\therefore \quad \underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{M}}\,d + \underline{\underline{I}}\,d^2$$

$$\therefore \quad [\underline{\underline{C}}(d)]^{-1} = \begin{bmatrix} 1+d^2 & d \\ d & 1+d+d^2 \end{bmatrix}^{-1} = \begin{bmatrix} 1+d+d^2 & d \\ d & 1+d^2 \end{bmatrix} \cdot \frac{1}{1+d+d^2+d^3+d^4}$$

Case (i) : $$= [\underline{\underline{I}} + \underline{\underline{M}}^2 d + \underline{\underline{I}} d^2]\ \frac{1+d}{1+d^5}$$

And $$\underline{P}(d) = \sum_{j=0}^{1} \sum_{i=1}^{2-j} \underline{\underline{C}}_{i+j} \cdot \underline{X}_i^{(0)}\, d^j = \underline{\underline{C}}_1 \cdot \underline{X}_1^{(0)} + \underline{\underline{C}}_2 \cdot \underline{X}_2^{(0)} + \underline{\underline{C}}_2 \cdot \underline{X}_1^{(0)} d$$

$$= \underline{\alpha} + \underline{1}\ d.$$

Autonomous response $\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot \underline{P}(d) = [\underline{\underline{I}} + \underline{\underline{M}}^2 d + \underline{\underline{I}} d^2] \cdot [\underline{\alpha} + \underline{1} d] \frac{1+d}{1+d^5}$

$$= \frac{\underline{\alpha} + \underline{\alpha} d + \underline{1} d^2 + \underline{1} d^4}{1+d^5}$$

or $$Y = \left\{ \begin{matrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{matrix} \right\}$$ with period 5.

The total response is

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot [\underline{P}(d) + \underline{U}(d)]$$

For convenience, we write

$$\underline{C}(d) = \underline{1} + \underline{\alpha} d + \underline{1} d^2$$

$$\therefore \underline{Y}(d) = \frac{\underline{\alpha} + \underline{1} d}{\underline{1} + \underline{\alpha} d + \underline{1} d^2} + \frac{\underline{1} + \underline{\alpha} d + \underline{\alpha} d^4 + \underline{\alpha}^2 d^5 + \underline{\alpha}^2 d^8 + \underline{1} d^9}{(\underline{1} + \underline{\alpha} d + \underline{1} d^2)(1+d^{12})}$$

The division by vector is permitted since they are elements of $GF(2^2)$. The second term is expanded into partial fractions as,

$$\frac{\underline{1} + \underline{\alpha} d + \underline{\alpha} d^4 + \underline{\alpha}^2 d^5 + \underline{\alpha}^2 d^8 + \underline{1} d^9}{(\underline{1} + \underline{\alpha} d + \underline{1} d^2)(1+d^{12})} = \frac{1}{(\underline{1} + \underline{\alpha} d + \underline{1} d^2)(\underline{1} + \underline{\alpha} d)^3}$$

$$= \frac{\underline{A} d + \underline{B}}{\underline{1} + \underline{\alpha} d + \underline{1} d^2} + \frac{\underline{C}}{1 + \underline{\alpha} d} + \frac{\underline{D}}{\underline{1} + \underline{\alpha}^2 d^2} + \frac{\underline{E}}{(\underline{1} + \underline{\alpha} d)^3} .$$

The values of $\underline{A}$, $\underline{B}$, $\underline{C}$, $\underline{D}$ and $\underline{E}$ are calculated to be,

$$\underline{A} = \underline{1} \; ; \; \underline{B} = \underline{\alpha} \; ; \; \underline{C} = \underline{\alpha} \; ; \; \underline{D} = \underline{\alpha} \; ; \; \underline{E} = \underline{\alpha}^2$$

Therefore

$$\underline{Y}(d) = \frac{\underline{\alpha} + \underline{1}d}{\underline{1} + \underline{\alpha}d + \underline{1}d^2} + \frac{\underline{\alpha} + \underline{1}d}{\underline{1} + \underline{\alpha}d + \underline{1}d^2} + \frac{\underline{\alpha}^2 + \underline{\alpha}^2 d + \underline{1}d^2}{(\underline{1} + \underline{\alpha}d)^3}$$

$$= \frac{\underline{\alpha}^2 + \underline{\alpha}^2 d + \underline{1}d^2}{(\underline{1}+\underline{\alpha}d)^3}$$

$$\therefore \underline{Y}(d) = \frac{\underline{\alpha}^2+\underline{\alpha}d+\underline{\alpha}d^3+\underline{1}d^4+\underline{\alpha}^2 d^5+\underline{\alpha}^2 d^7+\underline{\alpha}d^8+\underline{1}d^9+\underline{1}d^{11}}{1+d^{12}}$$

Therefore this is the critical state and output period is 12.

Case (ii) : $\underline{P}(d) = \sum_{j=0}^{1} \sum_{i=1}^{2-j} \underline{\underline{C}}_{i+j} \cdot \underline{X}_1^{(0)} d^j = \underline{\underline{I}} \cdot \underline{\alpha} + \underline{\underline{M}} \cdot \underline{\alpha}^2 + \underline{\underline{M}} \cdot \underline{\alpha} d$

$$= \underline{\alpha} + \underline{1} + \underline{\alpha}^2 d = \underline{\alpha}^2 + \underline{\alpha}^2 d.$$

Total response in this case becomes

$$\underline{Y}(d) = \frac{\underline{\alpha}^2+\underline{\alpha}^2 d}{\underline{1}+\underline{\alpha}d+\underline{1}d^2} + \frac{\underline{\alpha}+\underline{1}d}{1+\underline{\alpha}d+\underline{1}d^2} + \frac{\underline{\alpha}^2+\underline{\alpha}^2 d+\underline{1}d^2}{(\underline{1}+\underline{\alpha}d)^3}$$

$$= \frac{\underline{1}+\underline{\alpha}d}{\underline{1}+\underline{\alpha}d+\underline{1}d^2} + \frac{\underline{\alpha}^2+\underline{\alpha}^2 d+\underline{1}d^2}{(1+\underline{\alpha}d)^3} .$$

The first term has exponent 5 and therefore output period = LCM (5,12) = 60

Example 3.6 : Find the response of the LFSR circuit over $GF(2^2)$ whose connection polynomial is $\underline{C}(d) = \underline{1}+\underline{\alpha}^2 d$. The initial conditions and the input sequence $\underline{U}$ are same as in Example 3.5.

Here $[\underline{\underline{C}}(d)]^{-1} = [\underline{\underline{I}} + \underline{\underline{M}}^2 d]^{-1} = [\underline{\underline{I}} + \underline{\underline{M}} d] \frac{1}{1+d+d^2}$

$\therefore$ Exp. $[\underline{\underline{C}}(d)] = 3$ = Autonomous period,

$$\underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} \cdot [\underline{P}(d) + \underline{U}(d)]$$

Case (i) : $\underline{P}(d) = \underline{\alpha} + \underline{1}d$

$$\underline{Y}(d) = \frac{\underline{\alpha} + \underline{1}d}{\underline{1}+\underline{\alpha}^2 d} + \frac{1}{(\underline{1}+\underline{\alpha}^2 d)(\underline{1}+\underline{\alpha} d)^3}$$

$$= \frac{\underline{\alpha}+\underline{1}d}{\underline{1}+\underline{\alpha}^2 d} + \frac{1}{\underline{1}+\underline{\alpha}^2 d} + \frac{\underline{\alpha} d + \underline{\alpha} d^2}{(\underline{1}+\underline{\alpha} d)^3}$$

$$= \frac{\alpha^2 + \underline{1}d}{\underline{1}+\underline{\alpha}^2 d} + \frac{\underline{\alpha} d + \underline{\alpha} d^2}{(\underline{1}+\underline{\alpha} d)^3}.$$

Therefore output period is LCM $[\text{Exp } (\underline{1}+\underline{\alpha}^2 d), \text{ Exp } (\underline{1}+\underline{\alpha} d)^3]$

$$= \text{LCM } [3, 12] = 12$$

Case (ii) : $\underline{P}(d) = \underline{\alpha}^2 + \underline{\alpha}^2 d$.

In this case also, output period is 12.

Example 3.7 : Find the output period for $\underline{C}(d) = \underline{1}+\underline{\alpha}^2 d$ and

$$\underline{U}(d) = \frac{\underline{1}+\underline{\alpha} d+\underline{1} d^2+\underline{\alpha}^2 d^3+\underline{\alpha}^2 d^5+\underline{1} d^7+\underline{\alpha}^2 d^8+\underline{\alpha}^2 d^9+\underline{\alpha}\, d^{10}+\underline{\alpha}^2 d^{11}}{1+d^{12}}$$

Here $\underline{Y}(d) = \frac{\underline{P}(d)}{\underline{1}+\underline{\alpha}^2 d} + \frac{\underline{1}+\underline{\alpha} d+\underline{1} d^2+\underline{\alpha}^2 d^3+\underline{\alpha}^2 d^5+\underline{1} d^7+\underline{\alpha}^2 d^8+\underline{\alpha}^2 d^9+\underline{\alpha}\, d^{10}+\underline{\alpha}^2 d^{11}}{(\underline{1}+\underline{\alpha}^2 d)(1+d^{12})}$

And since $\underline{1} + \underline{\alpha}^2 d$ is a factor of $\underline{1} + \underline{1}\, d^{12}$, we cannot get partial

fraction of the type $\frac{\underline{A}(d)}{\underline{1} + \underline{\alpha}^2 d} + \frac{\underline{B}(d)}{\underline{1} + \underline{1}d^{12}}$.

Therefore output period = LCM $[\mathrm{Exp}(\underline{1}+\underline{\alpha}^2 d),\ \mathrm{Exp}((\underline{1}+\underline{\alpha}^2 d)\cdot(1+d^{12}))]$

$$= \mathrm{LCM}\ [3, 24]$$

$$= 24$$

Use of LFSR circuit as Scrambler :

In the calculation of period of output sequence for the case I of the LFSR circuit, we see that if the autonomous period and input sequence periods are relatively prime, then the output sequence period is the product of the two periods. Also, if the connection polynomial of the LFSR circuit is a primitive polynomial then the autonomous period is $(2^n)^m - 1$ and the output period in this case is $b\cdot(2^{nm}-1)$, where b is input sequence period. Thus the input sequence is translated into another with much extended period. It can also be verified that the number of transitions are more in the output sequence than in the input. Therefore such a circuit can be used for scrambling purposes. The difference between a binary scrambler and this scrambler is that this scrambler scrambles binary vector data.

CHAPTER IV

SYNTHESIS OF LFSR CIRCUITS OVER GF(2^n)

In this chapter synthesis procedure of a LFSR circuit which can generate a given vector sequence is given. In Section 4.1, the synthesis problem is explained. In Section 4.2, Massey's algorithm[8] is described and in Section 4.3, the overall synthesis procedure is explained with the help of appropriate flow charts. At the end of this chapter, a computer program is given which is based on the synthesis procedure described in Section 4.3. This program can be used to design LFSR circuits which can generate the given vector sequence. Examples of synthesis of a variety of vector sequences solved by using the given computer program are included.

4.1 The Synthesis problem: In this section, we give the synthesis problem and synthesize a LFSR circuit over GF(2^n) by a classical procedure. The problem arising in the synthesis procedure are described. We see that this procedure is very much involved. It has been proved[21] that among the various existing synthesis procedures, the Massey's synthesis procedure is the most efficient procedure, specially for synthesis over higher degree extension of fields.

Consider a finite length sequence of binary n x 1 vectors taken as elements of $GF(2^n)$

$$\underline{S}_{-1} = \underline{s}_o \underline{s}_{-1} \underline{s}_{-2} \cdots \underline{s}_{p-1}$$

$\underline{S}_{-1}$ may also be considered to consist of the initial P bits of the periodic sequence $\underline{S} = \underline{s}_o \underline{s}_{-1} \underline{s}_{-2} \cdots \underline{s}_{p-1}\ \underline{s}_o \underline{s}_{-1} \cdots$ with period P. On the other hand, if a given sequence is of infinite length then it is periodic. Therefore we have to design a LFSR circuit which can generate a vector sequence with arbitrary period.

The sequence $\underline{S}$ can be written in the polynomial form using Eq. 2.3-2 as

$$\underline{S}(d) = \frac{\underline{s}_o + \underline{s}_1 d + \underline{s}_2 d^2 + \cdots + \underline{s}_{p-1} d^{p-1}}{1+d^p}$$

$$= \frac{\underline{s}_o + \underline{s}_1 d + \underline{s}_2 d^2 \cdots + \underline{s}_{p-1} d^{p-1}}{\underline{1}+\underline{1}d^p}$$

The denominator $\underline{1} + \underline{1}d^p$ is obtained by dividing $\underline{S}(d)$ by the unit element of the field $\underline{1}$. The numerator and denominator of the above equation are polynomials in d over the field $GF(2^n)$ and can be factorized as,

$$\underline{s}_o + \underline{s}_1 d + \underline{s}_2 d^2 + \ldots + \ldots + \underline{s}_{p-1} d^{p-1} = \underline{f}_1(d)\ \ \underline{f}_2(d)\ \ \ldots \underline{f}_a(d)$$

$$\underline{1} + \underline{1}d^p = \underline{g}_1(d)\ \ \underline{g}_2(d)\ \ \ldots \underline{g}_b(d)$$

Where the multiplication of vectors is already defined. Some of the factors may be common to both the numerator and

denominator and can be cancelled. Therefore the expression for $\underline{S}(d)$ becomes

$$\underline{S}(d) = \frac{\underline{F}(d)}{\underline{G}(d)}, \text{ where } \underline{F}(d) \text{ and } \underline{G}(d) \text{ are relatively prime polynomials over } GF(2^n)$$

Thus the sequence $\underline{S}$ is represented by ratio of two relatively prime polynomials in d over $GF(2^n)$ and can be generated by a LFSR circuit over $GF(2^n)$ whose connection polynomial is $\underline{G}(d)$ and initial conditions are given by $\underline{F}(d)$.

Example 4.1. Find the connection polynomial of LFSR circuit which can generate the periodic sequence

$$\underline{S} = \left\{ \begin{matrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{matrix} \right\} \quad \text{with period 7.}$$

Choosing $\underline{\alpha} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ and $g(x) = 1+x^2+x^3$, the sequence can be written as,

$$\underline{S} = \underline{\alpha}^4\underline{\alpha}^3\underline{1}\ \underline{\alpha}\ \underline{\alpha}^2\underline{\alpha}^5\underline{\alpha}^6$$

$$\text{or } \underline{S}(d) = \frac{\underline{\alpha}^4 + \underline{\alpha}^3 d + \underline{1}d^2 + \underline{\alpha}d^3 + \underline{\alpha}^2 d^4 + \underline{\alpha}^5 d^5 + \underline{\alpha}^6 d^6}{\underline{1} + \underline{1}d^7}$$

and after going through a very lengthy process of determining the factors of numerator polynomial, we get

$$\underline{S}(d) = \frac{(\underline{\alpha} + \underline{\alpha}^3 x + \underline{\alpha}^6 x^2)(\underline{1} + \underline{1}x^2 + \underline{1}x^3 + \underline{1}x^4)}{(\underline{1} + \underline{1}x^2 + \underline{1}x^3 + \underline{1}x^4)(\underline{1} + \underline{1}x^2 + \underline{1}x^3)} = \frac{\underline{\alpha} + \underline{\alpha}^3 x + \underline{\alpha}^6 x^2}{\underline{1} + \underline{1}x^2 + \underline{1}x^3}$$

Therefore the given sequence eq. be generated by a 3 stage LFSR circuit whose connection polynomial is $\underline{1} + \underline{1}x^2 + \underline{1}x^3$.

If we choose $\underline{\beta} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$ and $q(x) = 1+x^2+x^3$, the sequence becomes

$\underline{S} = \underline{\beta}^3\underline{\beta}^4 1\ \underline{\beta}^6\underline{\beta}^5\underline{\beta}^2\underline{\beta}$ ... and the LFSR circuit has still 3 stage

However if we choose $q(x) = 1+x+x^3$, $\underline{\alpha} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ then

and $$\underline{S}(d) = \frac{\underline{\alpha}^5 + \underline{\alpha}^6 d + 1d^2 + \underline{\alpha} d^3 + \underline{\alpha}^2 d^4 + \underline{\alpha}^3 d^5 + \underline{\alpha}^4 d^6}{\underline{1}+\underline{1}d^7} = \frac{\underline{\alpha}^5}{\underline{1}+\underline{\alpha}d}$$

Thus a single stage LFSR circuit whose connection polynomial is $\underline{1}+\underline{\alpha}d$ can generate $\underline{S}$. From the above discussion, followed by an illustrative example, we observe that the design procedure involves the following steps.

1. Choose an irreducible polynomial $q(x)$ of degree n, and a primitive element $\underline{\alpha}$ among various possible choices.
2. Write the given sequence as a sequence of powers of $\underline{\alpha}$.
3. Write the sequence in polynomial form. Find the factors of numerator and denominator polynomials. Cancell common terms.
4. The resulting denominator polynomial is the connection polynomial of the desired LFSR circuit.
5. Calculate initial conditions from the numerator polynomial.

The above procedure has the following drawbacks.

1. Different choices of $\underline{\alpha}$ simply rename the sequence and the designed LFSR circuit is not changed, but different choices of $q(x)$ lead to different LFSR circuits and an arbitrary choice may not give the shortest length LFSR circuit.

2. A finite length sequence of length P may be portion of a periodic sequence of period $P_1 > P$ which may be generated by a LFSR circuit much shorter than the one which generates sequence with period P. But there is no way to know P_1. Therefore shortest length is not guaranted.

3. Factorization of polynomials is a difficult task. It becomes more difficult as we go to higher degree extension of fields.

The synthesis procedure given by Massey[8] is free from few of these drawbacks and is proved to be the most efficient procedure. A synthesis procedure based of Massey's is given in the next section. The problem of getting shortest LFSR circuit for various choices of $q(x)$ is overcome by designing for all $q(x)$ and choosing the shortest one.

4.2 Brief Description of Massey's Algorithm: In this section, the Massey's synthesis procedure is described in brief. The procedure is based upon the following theorem, which asserts that the shortest length LFSR circuit which can generate a given sequence can be synthesized in an iterative fashion given by the theorem.

Theorem. In any field, let $S_0 S_1 \ldots S_{p-1}$ be given. Under the initial conditions $\Lambda^{(o)}(x) = 1$; $B^{(o)}(x) = 1$ and $L_o = 0$. Let the following set of recursive equations be used to compute $\Lambda^{(p)}(x)$

$$\Delta_R = \sum_{j=0}^{R-1} \Lambda_j^{(R-1)} S_{R-j-1}$$

$$L_R = \delta_R(R-L_{R-1}) + (1-\delta_R)L_{R-1}$$

$$\begin{bmatrix} \Lambda^{(R)}(x) \\ B^{(R)}(x) \end{bmatrix} = \begin{bmatrix} 1 & -\Delta_R x \\ \Delta_R^{-1}\delta_R & (1-\delta_R)x \end{bmatrix} \cdot \begin{bmatrix} \Lambda^{(R-1)}(x) \\ B^{(R-1)}(x) \end{bmatrix} \qquad 4.1\text{-}1$$

$$R=1,2,\ldots P$$

where $\delta_R = 1$ if $\Delta_R \neq 0$ and $2L_{R-1} \quad R-1$

$\delta_R = 0$ otherwise

Then $\Lambda^{(P)}(x)$ is the smallest degree polynomial with the properties that

$$\Lambda_0^{(P)}(x) = 1 \qquad 4.1\text{-}2$$

and $$S_{R-1} + \sum_{j=1}^{R-1} \Lambda_j^{(P)} S_{R-j-1} = 0, \quad R = L_P+1, \ldots P$$

$\Delta_R^{-1}\delta_R$ is understood to be zero whenever $\Delta_R = \delta_R = 0$.

Now we see how the above theorem is useful for LFSR circuit synthesis. Let $\underline{S} = \underline{S}_0\underline{S}_1\underline{S}_2\ldots\underline{S}_{P-1}$ be some given vector sequence and a LFSR circuit is to be designed to generate it. If such a circuit is designed with tap coefficient $\underline{C}_1\ \underline{C}_2\ldots\underline{C}_{L_p}$ and has L_P number of stages then we can write Eq. 3.2-16 for this case as,

$$\underline{S}_k = \sum_{j=1}^{L_p} \underline{C}_j \underline{S}_{k-j} \quad , \quad k = L_p, L_p+1 \ldots P-1$$

$$= \sum_{j=1}^{L_p} \underline{\underline{C}}_j \underline{S}_{k-j} \quad , \quad k = L_p, L_p+1 \ldots P-1 \qquad 4.1\text{-}3$$

where the multiplication of vectors is defined in Sec. 2.2 and $\underline{\underline{C}}_j$ are matrices corresponding to vectors $\underline{C}_j$.

If the designed circuit is of shortest length then the polynomial

$$\underline{\underline{C}}(x) = \underline{\underline{C}}_0 + \underline{\underline{C}}_1 x + \underline{\underline{C}}_2 x^2 + \ldots + \underline{\underline{C}}_{L_p} x^{L_p}$$

must be a smallest degree polynomial with the properties that

$$\underline{\underline{C}}_0 = \underline{\underline{I}} \qquad 4.1\text{-}4$$

and $$\underline{S}_{k-1} + \sum_{j=1}^{k-1} \underline{\underline{C}}_j \underline{S}_{k-j-1} = \underline{\varphi} \quad k = L_p+1, \ldots P \quad \text{(using Eq. 4.1-3)}$$

And if we compare the above properties with those given by Eq. 4.1-2, we observe that these are the same.

Now we show how Eq. 4.1-1 can be used to calculate $\underline{\underline{C}}(x)$ so that $\underline{\underline{C}}(x)$ has the properties given by Eq. 4.1-4

The synthesis procedure based on Eq. 4.1-1 is iterative and consists of determination of the quantities L, which is the LFSR length and the connection polynomial $\underline{\underline{C}}(x)$ given by

$$\underline{\underline{C}}(x) = \underline{\underline{I}} + \underline{\underline{C}}_1 x + \underline{\underline{C}}_2 x^2 + \ldots + \ldots + \underline{\underline{C}}_L x^L .$$

This pair of quantities is denoted by $(L, \underline{\underline{C}}(x))$.

For each R, starting from R=1, a shortest LFSR circuit is designed for generating the first R elements of the sequence $\underline{S}$. The LFSR circuit given by $(L_R, \underline{\underline{C}}^{(R)}(x))$ is a minimum length circuit for producing $\underline{S}_0\underline{S}_1\underline{S}_2\cdots\underline{S}_{R-1}$. This LFSR circuit may not be unique. Several choices may exist, but all will have equal length. At the start of R^{th} iteration, a list of LFSR circuits $(L_i, \underline{\underline{C}}^{(i)}(x))$, i=1,2,...R-1 is constructed. The circuit $(L_{R-1}, \underline{\underline{C}}^{(R-1)}(x))$ can generate $\underline{S}_0\underline{S}_1\underline{S}_2\cdots\underline{S}_{R-2}$. The R^{th} output of this circuit is,

$$\underline{S}_{R-1} = \sum_{j=1}^{R-1} \underline{\underline{C}}_j^{(R-1)} \underline{S}_{R-j-1}$$

A quantity $\underline{\Delta}_R$, known as the R^{th} discrepency is obtained as,

$$\underline{\Delta}_R = \underline{S}_{R-1} - \underline{S}_{R-1} = \underline{S}_{R-1} + \sum_{j=1}^{R-1} \underline{\underline{C}}_j^{(R-1)} \cdot \underline{S}_{R-j-1}$$

or $$\underline{\Delta}_R = \sum_{j=0}^{R-1} \underline{\underline{C}}_j^{(R-1)} \cdot \underline{S}_{R-j-1}$$

If $\underline{\Delta}_R = \underline{\varphi}$, then the $(R-1)^{th}$ LFSR circuit can also generate the R^{th} element of the sequence $\underline{S}_{R-1}$, and then $(L_R, \underline{\underline{C}}^{(R)}(x)) = (L_{R-1}, \underline{\underline{C}}^{(R-1)}(x))$.

Otherwise the circuit taps are modified as follows,

$$\underline{\underline{C}}^{(R)}(x) = \underline{\underline{C}}^{(R-1)}(x) + \underline{\underline{A}}\, x^l\, \underline{\underline{C}}^{(m-1)}(x)$$

where $\underline{\underline{A}}$ is a field element (i.e. matrix equivalent of a field element $\underline{A}$), l is an integer and $\underline{\underline{C}}^{(m-1)}(x)$ is one of the LFSR polynomials calculated earlier.

A proper choice of $\underline{A} = \underline{\Delta}_n^{-1} \underline{\Delta}_R$ and $l = R-m$ gives

$$\underline{\underline{C}}^{(R)}(x) = \underline{\underline{C}}^{(R-1)}(x) + \underline{\Delta}_m^{-1} * \underline{\Delta}_R \, x * \underline{\underline{C}}^{(m-1)}(x)$$

and the new discrepency $\underline{\Delta}'_R$ becomes

$$\underline{\Delta}'_R = \sum_{j=0}^{R-1} \underline{\underline{C}}_j^{(R)} \underline{S}_{R-j-1}$$

$$= \sum_{j=0}^{R-1} \underline{\underline{C}}_j^{(R-1)} + \underline{\Delta}_m^{-1} \underline{\Delta}_R x * \sum_{j=0}^{R-1} \underline{\underline{C}}_j^{(m-1)} \underline{S}_{R-j-1}$$

$$= \underline{\Delta}_R + \underline{\Delta}_m^{-1} * \underline{\Delta}_R * \underline{\Delta}_m$$

$$= \underline{\varphi}$$

and therefore $\underline{\underline{C}}^{(R)}(x)$ can be used to generate $\underline{S}_{R-1}$.

In this manner, we start from $\underline{\underline{C}}^{(o)}(x) = \underline{\underline{I}}$, $L_o = 0$ and $\underline{\Delta}_{m_o} = \underline{1}$, $\underline{\underline{C}}^{(m_o-1)}(x) = \underline{\underline{I}}$ and proceed upto $R=P$ and thus calculate $(L_p, \underline{\underline{C}}^{(P)}(x))$ which is the shift register design for $\underline{S} = \underline{S}_o \underline{S}_1 \underline{S}_2 \cdots \underline{S}_{P-1}$.

We observe that the choices of $\underline{A}, l, \underline{\Delta}_{m_o}, \underline{\underline{C}}^{(m_o-1)}(x)$ in the above case are equivalent to determination of $\underline{\underline{C}}^{(P)}(x)$ using Eq. 4.1-1. Therefore the theorem ensures that $\underline{\underline{C}}^{(P)}(x)$ is the smallest degree polynomial with the properties given by Eq. 4
In determination of $\underline{C}(x)$ by using Eq. 4.1-4, a polynomial

$$\underline{\underline{B}}^{(R)}(x) = \underline{\Delta}_{m_R} * \underline{\underline{C}}^{(m_R-1)}(x)$$ is introduced

where $M_R < R$ is the largest integer such that $\delta_{m_R} = 1$, and δ is given by Eq. 4.1-1. In otherwords m_R is the most recent

iteration number in which length was changed, and this choice of m_R guarantees that $\underline{\underline{C}}(x)$ calculated by Eq. 4.1-1 is of shortest length.

4.3 The Synthesis Procedure: In the previous section, we have seen that the synthesis procedure involves multiplication and inversion of field elements. In the present case, the field element are represented by binary vectors, and their multiplication and inversion can not be achieved using ordinary rules. It has been discussed in Section 2.2, that for these purposes, the vectors are converted into corresponding matrices given by Eqs. 2.2-7, 2.2.8 and 2.2-9. Therefore whenever there is a multiplication or inversion of field elements in the calculation of $\underline{\underline{C}}(x)$, the elements are converted into corresponding matrices. The process of obtaining matrices corresponding to vectors is already discussed in Section 2.2. Here we represent it with the help of flow chart number 1.

Flow chart number 1 explains how multiplication and inversion of field elements is obtained. The synthesis procedure is explained with the help of flow chart number 2.

After the LFSR circuit given by $(L_p, \underline{\underline{C}}^{(P)}(x))$ is designed for one choice of $q_K^{(n)}(x)$, the other designs should be determined so as to choose the shortest LFSR among them. This can be achieved by following the procedure given by flow chart number 3. In this procedure, after calculation of $(L_p, \underline{\underline{C}}^{P}(x))$

for each choice of $q_K^{(n)}(x)$, K is increased by one and the process is continued. Simultaneously, the smallest number among the L_p's calculated for each K, is stored as the value of the variable LENGTH and corresponding $\underline{\underline{C}}(x)$ is stored in the name CON(x). This process terminates when all irreducible polynomials $q_K^{(n)}(x)$ has been considered. At the end of this chapter, a computer program in FORTRAN IV is given which can be used to calculate the connection polynomial and the number of stages of the LFSR circuit which can generate the sequence specified in the input file of the program. Because of memory limitations, this program is made to design LFSR circuits for generation of sequences of length less than 100 over the field $GF(2^n)$, where $n \leq 5$. However, it can easily be extended for higher values of n and P.

Few examples are solved with the help of the given computer program and it can be verified that the circuit is of shortest length in each case.

For simplicity of calculation of initial contents, the output is drawn from the last stage. Therefore the initial contents can be determined by using Eq. 3.3-7 and 3.3-8 and they coincide with the m initial bits of the given sequence.

i.e. For $\underline{S} = \underline{s}_0\underline{s}_1\underline{s}_2\underline{s}_3 \cdots \underline{s}_{P-1}$

The initial contents are

$$\underline{X}_1^{(o)} = \underline{S}_{m-1}$$

$$\underline{X}_2^{(o)} = \underline{S}_{m-2}$$

$$\underline{X}_3^{(o)} = \underline{S}_{m-3}$$

$$\vdots$$

$$\underline{X}_m^{(o)} = \underline{S}_o$$

However, if we want to draw output from the input point of first stage only then from Eq. 3.3-4

$$\underline{\underline{C}}(d)\ \underline{Y}(d) = \left[\sum_{j=0}^{m-1} \sum_{i=1}^{m-j} \underline{\underline{C}}_{i+j} \cdot \underline{X}_i^{(o)} d^j \right]$$

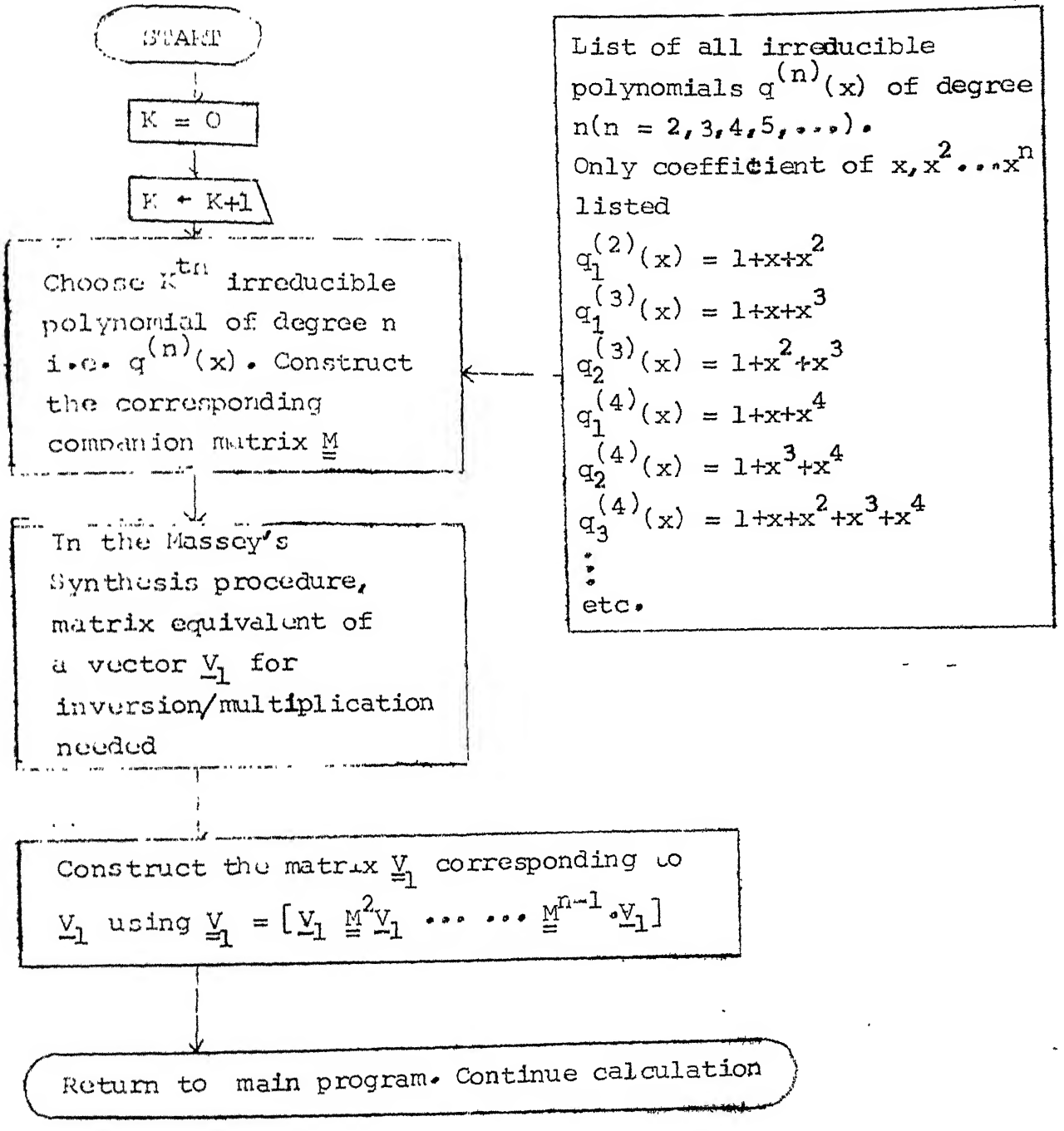
or writing first m elements of the sequence $\underline{Y}$ given by

$$\underline{Y}(d) = \frac{\underline{Y}_o + \underline{Y}_1 d + \underline{Y}_2 d^2 + \ldots + \underline{Y}_{p-1} d^{P-1}}{1+d^P}$$ in matrix form

$$\begin{bmatrix} \underline{\underline{I}} & \underline{\underline{\varphi}} & \underline{\underline{\varphi}} & \cdots & \underline{\underline{\varphi}} \\ \underline{\underline{C}}_1 & \underline{\underline{I}} & \underline{\underline{\varphi}} & \cdots & \underline{\underline{\varphi}} \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ \underline{\underline{C}}_{m-1} & \underline{\underline{C}}_{m-2} & \underline{\underline{C}}_{m-3} & \cdots & \underline{\underline{I}} \end{bmatrix} \cdot \begin{bmatrix} \underline{Y}_o \\ \underline{Y}_1 \\ \underline{Y}_2 \\ \cdot \\ \cdot \\ \underline{Y}_{m-1} \end{bmatrix} \quad \begin{bmatrix} \underline{\underline{C}}_1 & \underline{\underline{C}}_2 & \cdots & \underline{\underline{C}}_m \\ \underline{\underline{C}}_2 & \underline{\underline{C}}_3 & \cdots & \underline{\underline{\varphi}} \\ \cdot & & & \cdot \\ \cdot & & & \cdot \\ \underline{\underline{C}}_m & \underline{\underline{\varphi}} & \cdots & \underline{\underline{\varphi}} \end{bmatrix} \cdot \begin{bmatrix} \underline{X}_1^{(o)} \\ \underline{X}_2^{(o)} \\ \cdot \\ \cdot \\ \underline{X}_m^{(o)} \end{bmatrix}$$

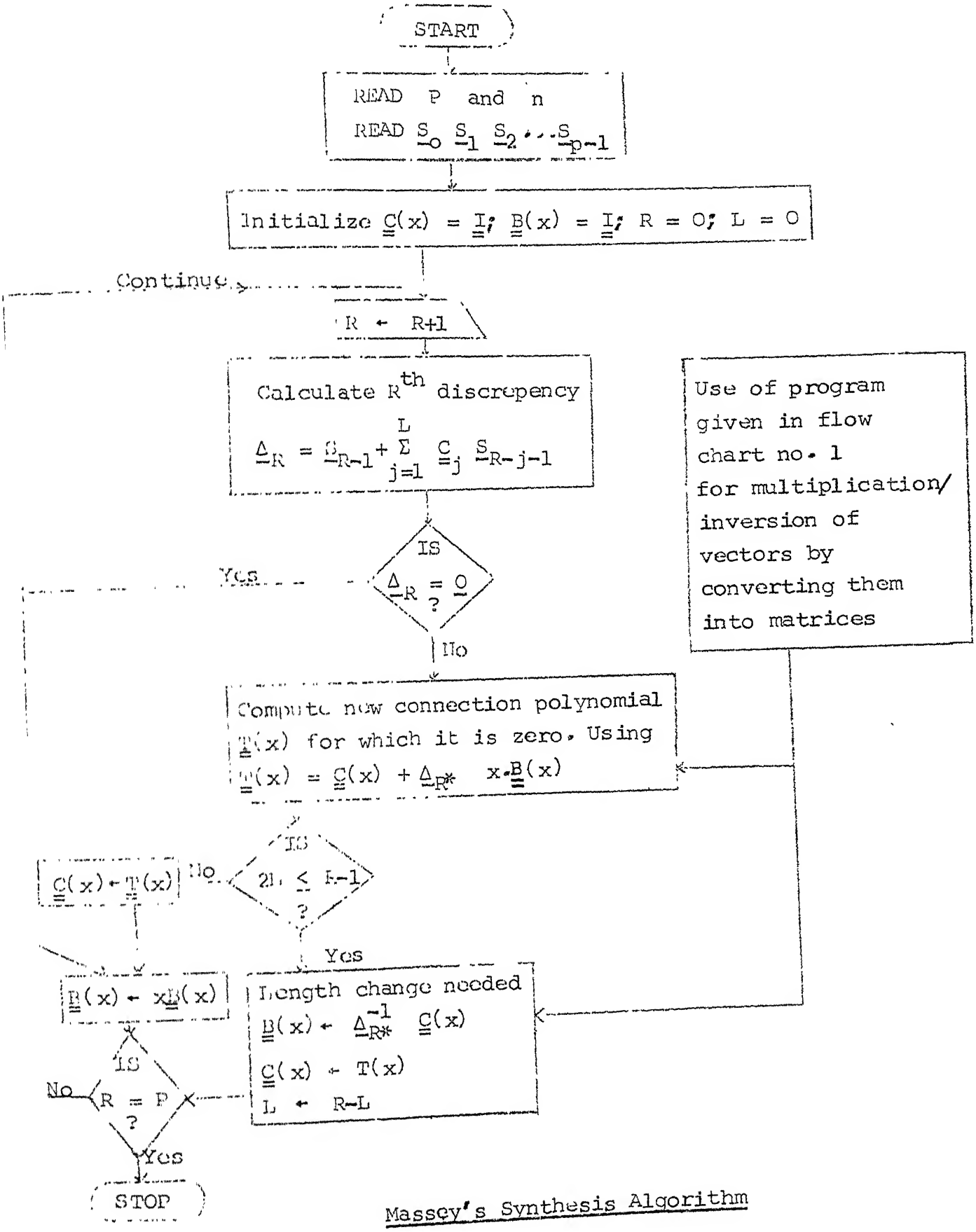
And therefore $\underline{X}_1^{(o)}, \underline{X}_2^{(o)} \ldots \underline{X}_m^{(o)}$ can be calculated in terms of $\underline{\underline{C}}_1\ \underline{\underline{C}}_2 \cdots \underline{\underline{C}}_m$ and $\underline{Y}_o\ \underline{Y}_1 \cdots \underline{Y}_{m-1}$.

FLOW CHART NO. 1



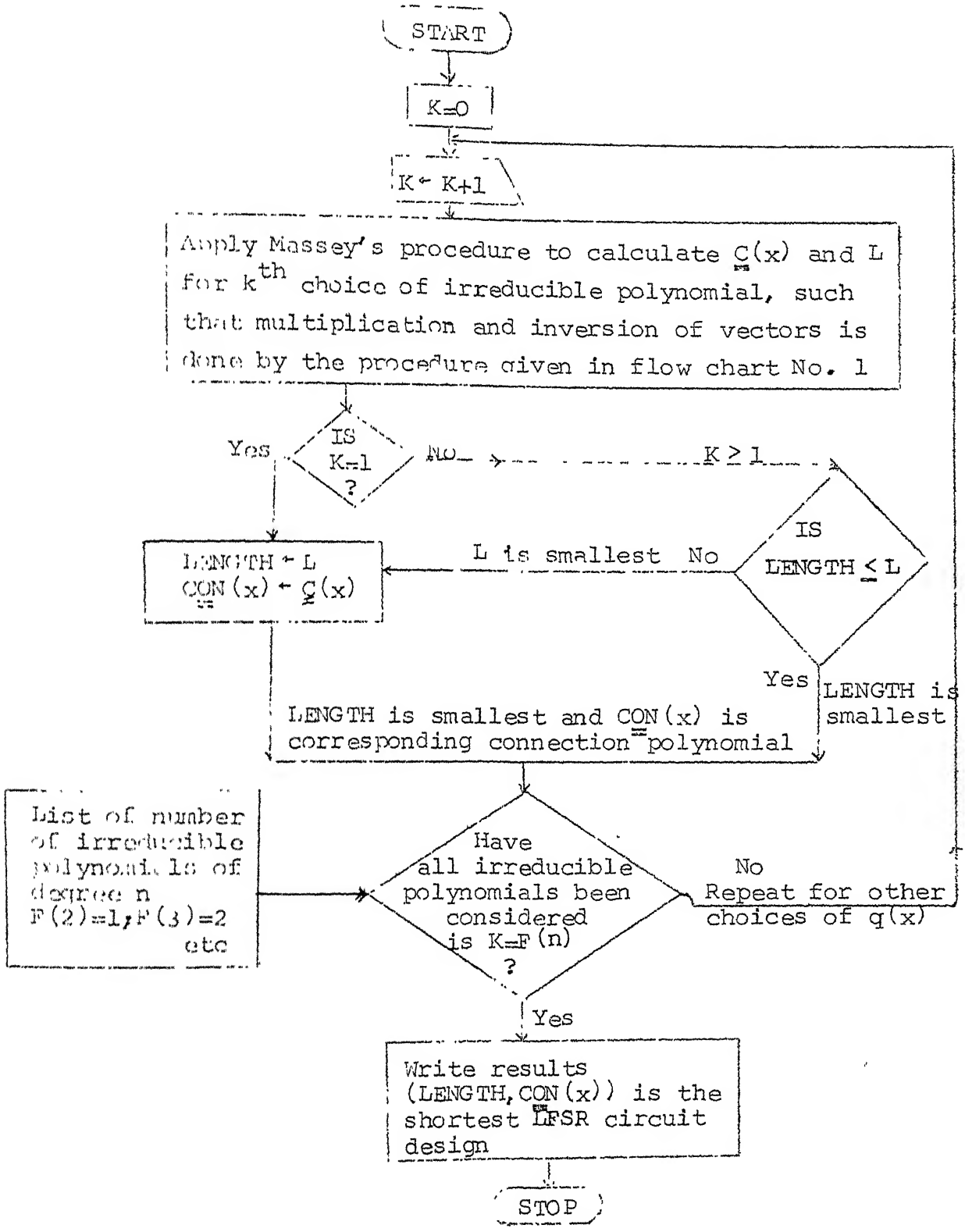
Procedure to obtain matrix corresponding to some vector.

FLOW CHART NO. 2



Massey's Synthesis Algorithm

FLOW CHART NO. 3



Synthesis procedure with provision to choose the shortest LFSR circuit

In the following example, a LFSR circuit is designed to generate a given sequence. The example is solved in detail, showing at each step, the values of various variables used in the computer program. The symbols used here are the same as are used in the program. Then few more examples are given which are solved with the help of computer, and only the results are given.

Example 4.2

Synthesize a LFSR circuit to generate the sequence over $GF(z^3)$

$$\left\{\begin{matrix}1110100\\0111010\\0100111\end{matrix}\right\}$$ with sequence length 7.

Solution. Various variables are declared integer and are dimensioned. The read statement assigns,

P = 7 ; N = 3

S(1,1)=1; S(1,2)=1; S(1,3)=1; S(1,4)=0; S(1,5)=1; S(1,6)=0; S(1,7)=

S(2,1)=0; S(2,2)=1; S(2,3)=1; S(2,4)=1; S(2,5)=0; S(2,6)=1; S(2,7)=

S(3,1)=0; S(3,2)=1; S(3,3)=0; S(3,4)=0; S(3,5)=1; S(3,6)=1; S(3,7)=

Companion matrix corresponding to 3rd degree polynomial for K=1 is formed. Thus

$$\underline{\underline{M}} = \begin{bmatrix}0 & 0 & 1\\1 & 0 & 1\\0 & 1 & 0\end{bmatrix}$$

Massey's Algorithm Starts. Initialization.

$R=0;\ L=0;\ \underline{\underline{B}}(1) = \underline{\underline{B}}(2) = \ldots = \underline{\underline{B}}(P) = \underline{\underline{O}}\ ;\ \underline{\underline{LEM}}(1) = \underline{\underline{LEM}}(2) = \ldots \underline{\underline{LEM}}(P) = \underline{\underline{O}}$

$$\underline{\underline{B}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \underline{\underline{LEM}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The values of the various variables for each iteration are tabulated below

R=1

$$\underline{DEL}(1) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} ;\ \overset{(1)}{\underline{\underline{T}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \overset{(1)}{\underline{\underline{T}}}(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$2L \leq R-1;\ \overset{(1)}{\underline{\underline{B}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \overset{(1)}{\underline{\underline{B}}}(2) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ;$

$$\overset{(1)}{\underline{\underline{LEM}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \overset{(1)}{\underline{\underline{LEM}}}(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ L=1$$

R=2

$$\underline{DEL}(2) = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} ;\ \overset{(2)}{\underline{\underline{T}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \overset{(2)}{\underline{\underline{T}}}(2) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

$2L > R-1\ ;\ \overset{(2)}{\underline{\underline{LEM}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ;\ \overset{(2)}{\underline{\underline{LEM}}}(2) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} ;$

$$\overset{(2)}{\underline{\underline{B}}}(1) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ;\ \overset{(2)}{\underline{\underline{B}}}(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

R=3

$$\underline{\underline{DEL}}(3) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad ; \quad \underline{\underline{DEL}}(R) = \underline{\underline{0}}$$

$$\therefore \underline{\underline{B}}^{(2)}(1) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ; \underline{\underline{B}}^{(2)}(2) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ;$$

$$\underline{\underline{B}}^{(3)}(3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ; \underline{\underline{LEM}}^{(3)} = \underline{\underline{LEM}}^{(2)}$$

R=4

$$\underline{\underline{DEL}}(4) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad ; \quad \underline{\underline{DEL}}(R) = \underline{\underline{0}}$$

$$\therefore \underline{\underline{B}}^{(4)}(4) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ; \underline{\underline{B}}^{(4)}(1) = \underline{\underline{B}}^{(4)}(2) = \underline{\underline{B}}^{(4)}(3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} ;$$

$$\underline{\underline{LEM}}^{(4)} = \underline{\underline{LEM}}^{(3)}$$

R=5

$$DEL(5) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad ; \quad \underline{\underline{DEL}}(R) = \underline{\underline{0}}$$

$$\therefore \underline{\underline{B}}^{(5)}(5) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} ; \underline{\underline{B}}^{(5)}(1) = \underline{\underline{B}}^{(5)}(2) = \underline{\underline{B}}^{(5)}(3) = \underline{\underline{B}}^{(5)}(4) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\underline{\underline{LEM}}^{(5)} = \underline{\underline{LEM}}^{(6)}$$

$$\underline{DEL}(6) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad \underline{DEL}(R) = \underline{0}$$

$$\therefore \overset{(6)}{\underline{\underline{B}}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad \overset{(6)}{\underline{\underline{B}}}(1) = \overset{(6)}{\underline{\underline{B}}}(2) = \overset{(6)}{\underline{\underline{B}}}(3) = \overset{(6)}{\underline{\underline{B}}}(4)$$

$$= \overset{(6)}{\underline{\underline{B}}}(5) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}; \quad \overset{(6)}{\underline{\underline{LEM}}} = \overset{(5)}{\underline{\underline{LEM}}}$$

K=7

$$\underline{DEL}(7) = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad \underline{DEL}(R) = \underline{0}$$

$$\therefore \overset{(7)}{\underline{\underline{B}}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad \overset{(7)}{\underline{\underline{B}}}(I) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad I = 1 \text{ to } 6$$

$$\overset{(7)}{\underline{\underline{LEM}}} = \overset{(6)}{\underline{\underline{LEM}}}; \quad L^{(7)} = L^{(2)} = 1$$

All syndromes are over, $F(N) = F(3)$ = Number of irreducible polynomials of degree 3 is 2.

Repeat the process for K=2 i.e. $\underline{\underline{M}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

In this case, final result is

L=3 and

$$\overset{(7)}{\underline{\underline{LEM}}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad \overset{(7)}{\underline{\underline{LEM}}}(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$\overset{(7)}{\underline{\underline{LEM}}}(3) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}; \quad \overset{(7)}{\underline{\underline{LEM}}}(4) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Therefore the last part of program chooses

$$\text{LENGTH} = 1 \qquad \underline{\underline{CON}}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \; ; \quad \underline{\underline{CON}}(2) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

The final answer is therefore,

$$\underline{\underline{CON}}(d) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \cdot d$$

The computer program and some examples solved by using it are given in the following pages.

```
      DIMENSION S(5,100),A(6,5,5),F(5),B(5,5,100)
     1,DEL(5,100),DELLL(5),BBB(5,5,100),BB(5,5)
     2,SUB(5,5,100),CON(5,5,100),SUM(5),SMAT1(5)
     3,T(5,5,100),DELBB(5,5),DELL(5,5)
     4,IBB(5,5),AAA(5,5),INVDEL(5,5),DEM1(5,5)
     1,BBB(5,5,100),DEMMAT(5),INDDUM(5,5),DEMMMM(5,5)
     2,IBBBB(5,5,100)
      OPEN(UNIT=3,DEVICE='DSK',FILE='SEQIN')
      OPEN(UNIT=1,DEVICE='DSK',FILE='RESULT')
      READ(3,*) P,N
      READ(3,*)((S(I,J),J=1,P),I=1,N)
      WRITE(1,201)
      WRITE(1,202)
      WRITE(1,203)
      OPEN(UNIT=8,DEVICE='DSK',FILE='SEQIN')
      DO 301 I=1,N
301   WRITE(1,204)(S(I,J),J=1,P)
      WRITE(1,205) P
201   FORMAT(16X,'Example',5X,'Design a LFSR circuit to generate')
203   FORMAT(32X,'the sequence'/)
202   FORMAT(16X,11('-'),/)
204   FORMAT(20X,10011,/)
205   FORMAT(32X,'with sequence length  ',I3,'.',///)
C     COEFFICIENTS OF POWERS OF X IN PRIMITIVE POLYNOMIAL OF
C     DEGREE 1 THROUGH 5
      A(1,2,2)=1
      A(1,3,2)=1;A(1,3,3)=0
      A(2,3,2)=0;A(2,3,3)=1
      A(1,4,2)=1;A(1,4,3)=0;A(1,4,4)=0
      A(2,4,2)=0;A(2,4,3)=0;A(2,4,4)=1
      A(3,4,2)=1;A(3,4,3)=1;A(3,4,4)=1
      A(1,5,2)=0;A(1,5,3)=1;A(1,5,4)=0;A(1,5,5)=0
      A(2,5,2)=0;A(2,5,3)=0;A(2,5,4)=1;A(2,5,5)=0
      A(3,5,2)=1;A(3,5,3)=1;A(3,5,4)=1;A(3,5,5)=0
      A(4,5,2)=1;A(4,5,3)=1;A(4,5,4)=0;A(4,5,5)=1
      A(5,5,2)=1;A(5,5,3)=0;A(5,5,4)=1;A(5,5,5)=1
      A(6,5,2)=0;A(6,5,3)=1;A(6,5,4)=1;A(6,5,5)=1
      F(1)=1;F(2)=1;F(3)=2;F(4)=3;F(5)=6
      K=0
2     K=K+1
C     FORMATION OF COMPANION MATRIX CORRESPONDING TO
C     K'th PRIMITIVE POLYNOMIAL
      DO 3 I=1,N
      DO 3 J=1,N-1
      M(I,J)=0
      IF(I-J.EQ.1) B(I,J)=1
3     CONTINUE
      DO 4 I=2,N
4     M(I,N)=A(K,N,1)
      M(1,N)=1
C     *****   MASSEY'S  ALGORITHM  STARTS  HERE  *****
C     INITIALIZATION
      R=0
      L=0
      DO 141 I=1,N
      DO 141 J=1,N
      DO 141 II=1,P
      LEN(I,J,II)=0
141   B(I,J,II)=0
      DO 21 I=1,N
      DO 21 J=1,N
      IF(I-J) 22,23,22
22    B(I,J,1)=0
      LEN(I,J,1)=0;GOTO 21
23    B(I,J,1)=1
      LEN(I,J,1)=1
21    CONTINUE
C     CALCULATION OF R'th DISCREPENCY
C     DELTA(R)=SMAT(R)+SUMMATION(J=1to L)LEN(J+1)*SMAT(R-J)
24    R=R+1
```

```
      DO 25 I=1,J
25    DEL(I,R)=S(L,R)
      IF(L.L).0) GOTO 30
      DO 26 I=1,N
26    SUM(I)=0
      DO 47 JJ=1,L
      J1=J-JJ
      DO 28 I=1,N
      SMAT1(I)=S(I,J1)
      DO 28 J=1,N
28    LEM1(I,J)=LEM(I,J,JJ+1)
      CALL MATVCT(LEM1,SMAT1,LEMMAT,N)
      DO 27 I=1,N
27    SUM(I)=ABS(SUM(I)-LEMMAT(I))
      DO 29 I=1,N
29    DEL(I,R)=ABS(DEL(I,R)-SUM(I))
C     IS R'th DISCREPENCY ZERO?
30    DO 32 I=1,N
      IF(DEL(I,R)) 33,32,33
32    CONTINUE
      GOTO 44
C     DELTA(R) IS NONZERO.
CC    CALCULATE NEW CONNECTION POLYNOMIAL
CC    FOR WHICH DELTA(R) IS ZERO.
C     T(x)=LEM(x)+DEL(R)*B(x)*x
33    DO 31 I=1,N
31    DELLLL(I)=DEL(I,R)
      CALL VETMAT(DELLLL,N,DELL,N)
      DO 36 I1=2,R+1
      DO 37 I=1,N
      DO 37 J=1,N
37    BB(I,J)=B(I,J,I1-1)
      CALL MATMUT(DELL,BB,DELBB,N)
      DO 36 I=1,N
      DO 36 J=1,N
      DELB(I,J,I1)=DELBB(I,J)
36    T(I,J,I1)=ABS(LEM(I,J,I1)-DELB(I,J,I1))
      DO 38 I=1,N
      DO 38 J=1,N
38    T(I,J,1)=LEM(I,J,1)
C     IS LENGTH CHANGE NEEDED?
      IF(2*L-R+1) 40,40,41
C     2*L IS MORE THAN R-1.
CC    LEM(x)=T(x)
41    DO 43 I1=1,R+1
      DO 43 I=1,N
      DO 43 J=1,N
43    LEM(I,J,I1)=T(I,J,I1)
C     DELTA(R) IS ZERO,
CC    OR 2*L IS MORE THAN R-1.
C     B(x) <-----  x*B(x)
44    DO 45 I1=2,R+1
      DO 45 I=1,N
      DO 45 J=1,N
45    BBB(I,J,I1)=B(I,J,I1-1)
      DO 46 I=1,N
      DO 46 J=1,N
46    BBB(I,J,1)=0
      DO 47 I1=1,R+1
      DO 47 I=1,N
      DO 47 J=1,N
47    B(I,J,I1)=BBB(I,J,I1)
      GOTO 51
C     2*L IS LESS THAN/EQUAL TO R-1.
CC    B(x)=DELTA(R)INVERSE*LEM(x)
CC    LEM(x)=T(x)
C     L=R-L
40    DO 71 I9=1,N
      DO 71 J9=1,N
71    AAA(I9,J9)=DELL(I9,J9)
```

```
      CALL MATINV(AAA,N,BB,0,DET,5)
      DO 72 I8=1,N
      DO 72 J8=1,N
      RAAA=ABS(AAA(I8,J8))
      INTA=RAAA/2.
      RELA=RAAA/2.
      RELB=INTA
      IF(RELA-RELB) 73,74,73
73    IIA=1;GOTO 75
74    IIA=0
75    INVDEL(I8,J8)=IIA
72    CONTINUE
      DO 49 I1=1,R+1
      DO 50 I=1,N
      DO 50 J=1,N
50    LEMMMM(I,J)=LEM(I,J,I1)
      CALL MATMUT(INVDEL,LEMMMM,INDDDM,N)
      DO 49 I=1,N
      DO 49 J=1,N
      INDELM(I,J,I1)=INDDDM(I,J)
      B(I,J,I1)=INDELM(I,J,I1)
49    LEM(I,J,I1)=T(I,J,I1)
      L=P-L
C     ARE ALL SYNDROMES OVER?
51    IF(K.NE.P) GOTO 24
C     LENGTH=L FOR FIRST PRIMITIVE POLYNOMIAL.
C     CON(x)=LEM(x) FOR FIRST PRIMITIVE POLYNOMIAL.
      IF(K-1) 143,143,144
143   LENGTH=L
      DO 145 I=1,N
      DO 145 J=1,N
      DO 145 I1=1,R
145   CON(I,J,I1)=LEM(I,J,I1)
C     CALCULATE L & LEM(x) FOR OTHER PRIMITIVE POLYNOMIALS.
C     IF ODD LENGTH IS MORE THAN NEW LENGTH L THEN
C     LENGTH=NEW LENGTH L & CON(x)=NEW LEM(x)
      GOTO 147
144   IF(LENGTH-L) 147,147,146
146   LENGTH=L
      DO 148 I=1,N
      DO 148 J=1,N
      DO 148 I1=1,R
148   CON(I,J,I1)=LEM(I,J,I1)
C     TRY FOR OTHER PRIMITIVE POLYNOMIALS.
147   IF(K.NE.F(N)) GOTO 2
C     ALL PRIMITIVE POLYNOMIALS ARE OVER. WRITE RESULTS.
      WRITE(1,640)
      WRITE(1,639)
      WRITE(1,641) LENGTH
      WRITE(1,642)
640   FORMAT(16X,'RESULT')
639   FORMAT(16X,6('-'),/)
641   FORMAT(20X,'The designed LFSR Circuit has',I3,'   stages.')
642   FORMAT(20X,'Coefficients of the connection polynomial are:')
      DO 540 I1=1,LENGTH+1
      WRITE(1,644) I1
644   FORMAT(20X,I3,/)
      DO 540 I=1,N
      WRITE(1,204)(CON(I,J,I1),J=1,N)
540   CONTINUE
      STOP
      END
C     ***************************************************************
```

```
      SUBROUTINE MATINV(A,N,B,M,DETERM,NDIMEN)
      DIMENSION A(NDIMEN,NDIMEN),B(NDIMEN,1),IPIVOT(100),INDEX(100,2)
      DIMENSION DT(100)
      EQUIVALENCE (IROW,JROW),(ICOLUM,JCOLUM),(AMAX,T,SWAP)
10    DETERM=1.0
15    DO 20 J=1,N
20    IPIVOT(J)=0
30    DO 550 I=1,N
40    AMAX=0.0
45    DO 105 J=1,N
50    IF(IPIVOT(J)-1) 60,105,60
60    DO 100 K=1,N
70    IF(IPIVOT(K)-1) 80,100,740
80    IF(AMAX-ABS(A(J,K))) 85,100,100
85    IROW=J
90    ICOLUM=K
95    AMAX=ABS(A(J,K))
100   CONTINUE
105   CONTINUE
110   IPIVOT(ICOLUM)=IPIVOT(ICOLUM)+1
130   IF(IROW-ICOLUM)140,260,140
140   DETERM=-DETERM
150   DO 200 L=1,N
160   SWAP=A(IROW,L)
170   A(IROW,L)=A(ICOLUM,L)
200   A(ICOLUM,L)=SWAP
205   IF(M)260,260,210
210   DO 250 L=1,M
220   SWAP=B(IROW,L)
230   B(IROW,L)=B(ICOLUM,L)
250   B(ICOLUM,L)=SWAP
260   INDEX(I,1)=IROW
270   INDEX(I,2)=ICOLUM
310   PIVOT=A(ICOLUM,ICOLUM)
320   DT(I)=PIVOT
330   A(ICOLUM,ICOLUM)=1.0
340   DO 350 L=1,N
350   A(ICOLUM,L)=A(ICOLUM,L)/PIVOT
355   IF(M) 380,380,360
360   DO 370 L=1,M
370   B(ICOLUM,L)=B(ICOLUM,L)/PIVOT
380   DO 550 L1=1,N
390   IF(L1-ICOLUM) 400,550,400
400   T=A(L1,ICOLUM)
420   A(L1,ICOLUM)=0.0
430   DO 450 L=1,N
450   A(L1,L)=A(L1,L)-A(ICOLUM,L)*T
455   IF( M) 550,550,460
460   DO 500 L=1,M
500   B(L1,L)=B(L1,L)-B(ICOLUM,L)*T
550   CONTINUE
600   DO 710 I=1,N
610   L=N+1-I
      DETERM=DETERM*DT(L)
620   IF(INDEX(L,1)-INDEX(L,2)) 630,710,630
630   JROW=INDEX(L,1)
640   JCOLUM=INDEX(L,2)
650   DO 705 K=1,N
660   SWAP=A(K,JROW)
670   A(K,JROW)=A(K,JCOLUM)
700   A(K,JCOLUM)=SWAP
705   CONTINUE
710   CONTINUE
      DO 11 K=1,N
      IF(IPIVOT(K).NE.1) GOTO 12
11    CONTINUE
      RETURN
12    TYPE 991
991   FORMAT(10X,18HMATRIX IS SINGULAR  /)
740   RETURN
      END
```

```
C       ************************************************
        SUBROUTINE VETMAT(V,N,MAT,M)
        INTEGER M(5,5),MAT(5,5),V(5),V1(5),V2(5)
        DO 171 I=1,M
        MAT(I,1)=V(I)
171     V1(I)=V(I)
        DO 172 J=2,M
        CALL MATVET(M,V1,V2,M)
        DO 172 I=1,M
        V1(I)=V2(I)
172     MAT(I,J)=V2(I)
        RETURN
        END
C       ************************************************
C       SUBROUTINE FOR MULTIPLICATION OF A MATRIX BY A MATRIX
C       ORDER OF BOTH MATRICES IS N. ADDITION IS MODULO-2.
        SUBROUTINE MATMUT(M1,M2,M12,N)
        DIMENSION M12(5,5),M1(5,5),M2(5,5)
        DO 5 I=1,N
        DO 5 J=1,N
        LL=0
        DO 4 K=1,N
4       LL=ABS(LL-M1(I,K)*M2(K,J))
5       M12(I,J)=LL
        RETURN;END
C       ************************************************
C       SUBROUTINE TO MULTIPLY A MATRIX BY A VECTOR
        SUBROUTINE MATVET(A,B,X,N)
        INTEGER A(5,5),B(5),X(5)
        DO 55 I=1,N
        ISUM=0
        DO 45 K=1,N
45      ISUM=ABS(ISUM-A(I,K)*B(K))
55      X(I)=ISUM
        RETURN
        END
C       ************************************************
```

Example 4.3 Design a LFSR circuit to generate

the sequence

1001011000101001111011001110010010110111011001101010111111100000
0100111001011011101110011010101111110000010000110001010011110 1
with sequence length 63.

RESULT

The designed LFSR Circuit has 3 stages.
Coefficients of the connection polynomial are:
1

10
01
2

10
01
3

11
10
4

01
11

Example 4.4 Design a LFSR circuit to generate

the sequence

1111001001010100110100001000101101111110101110001100111011000001
1010100110100001000101101111110101110001100111011000001111001001
1101010111000110011101100000111100100101010011010000100010110111
with sequence length 63.

RESULT

The designed LFSR Circuit has 2 stages.
Coefficients of the connection polynomial are:
1

100
010
001
2

111
100
110
3

010
011
101

Example 4.5 Design a LFSR circuit to generate

the sequence

1111001001010100110100001000101101111101011100011001110110000

0011001111011000031111001001010100110100001000101101111101011

with sequence length 63.

Solution

The designed LFSR circuit has 6 stages.
Coefficients of the connection polynomial are:
1

100
010
001
2

100
010
001
3

100
000
000
4

100
000
000
5

100
010
001
6

100
010
101
7

100
010
101

Example 4.6 Design a LFSR circuit to generate

the sequence

1001011011111110110100100000
0111110000011111000011111000
0000101100110100000010110011101
0000100110111111110110100100
with sequence length 30.

RESULT

The designed LFSR Circuit has 5 stages.
Coefficients of the connection polynomial are:

1

1000
0100
0010
0001

2

0100
0110
0011
1001

3

1011
1110
1111
0111

4

1101
1011
0101
1010

5

1001
1101
0110
0011

6

1001
1101
0110
0011

7

1010
0111
1011
0101

Example 4.7 Design a LFSR circuit to generate

the sequence

111101011001000
011110101100100
001111010110010
100111101011001
110011110101100
111001111010110
011100111101011
101110011110101
010111001111010
001011100111101
100101110011110
010010111001111
101001011100111
110100101110011
111010010111001

with sequence length 15.

RESULT

The designed LFSR Circuit has 4 stages.
Coefficients of the connection polynomial are:
1

1000
0100
0010
0001
2

0001
1000
0100
0011

Example 4.8 Design a LFSR circuit to generate

the sequence

101011101100011
010101110110001
001010111011000
100111011000111
010011101100011
101001110110001
110100111011000
011010011101100
001101001110110
000110100111011
100011010011101
010001101001110
001000110100111
100100011010011
110010001101001

with sequence length 15.

RESULT

The designed LFSR Circuit has 4 stages.
Coefficients of the connection polynomial are:
1

10000
01000
00100
00010
00001
2

00001
10000
01000
00101
00010

CHAPTER V

CONCLUSION

In this thesis we have studied LFSR circuits over $GF(2^n)$ with the following two objectives. The first objective is: given a LFSR circuit, to obtain expressions for autonomous and total response of this circuit, and study the properties of the generated sequences. The second objective is: for a given sequence over $GF(2^n)$, to design a shortest length LFSR circuit which can generate it. Results obtained in the thesis are summarized in this chapter; some suggestions for further investigation in related area are also given.

The important results obtained from the analysis of LFSR circuits over $GF(2^n)$ are:

(1) Expressions for autonomous and total response of LFSR circuits over $GF(2^n)$ are similar to those for the case of LFSR circuits over $GF(2)$ except that the coefficients of various polynomials in the expressions are elements of $GF(2^n)$. Since the elements of $GF(2^n)$ are represented by n x 1 binary vectors, the division by the connection polynomial $\underline{C}(d)$ in the expressions corresponds to multiplication by $[\underline{C}(d)]^{-1}$, where $\underline{C}(d)$ is obtained by converting

vector coefficients of $\underline{\underline{C}}(d)$ into matrices. Thus the expression for the total response of LFSR circuits for GF(2) and GF(2^n) are:

$$GF(2) : Y(d) = \frac{P(d) + U(d)}{C(d)}$$

$$GF(2^n): \underline{Y}(d) = [\underline{\underline{C}}(d)]^{-1} [\underline{P}(d)+\underline{U}(d)]$$

where symbols have their usual meaning. The periods of output sequence in the case of GF(2^n) can be determined by using the procedure for GF(2).

(2) Individual rows of the sequences over GF(2^n) are binary sequences. For periodic vector sequences, these row sequences may have different periods such that their LCM is equal to the period of the vector sequence, but when the sequence is a maximal sequence row sequences are also maximal sequences with equal periods.

(3) In the case of maximal sequences, individual rows are shifted versions of the same binary sequence which can be generated by a mn stage binary LFSR circuit. The connection polynomial of this binary LFSR circuit is equal to the determinant of the matrix $\underline{\underline{C}}(d)$, which is the connection polynomial of the LFSR circuit over GF(2^n).

(4) The amounts by which rows of a maximal sequence are shifted from one of its rows (say from first row) are integral

multiples of a number $\beta = \frac{2^{mn}-1}{2^n-1}$, where m is number of stages in the LFSR.

(5) If the coefficients of a primitive polynomial over $GF(2^n)$ are raised to 2^{-j} power, where $j=1,2,3...n-1$, then the amounts of shifts for the sequence generated by this polynomial are 2^j times the amounts of shifts for the sequence generated by original polynomial.

For synthesis of LFSR circuits over $GF(2^n)$, we observe that:

1. LFSR circuits over $GF(2^n)$ can be synthesized by using Massey's algorithm.

2. Different choices of the irreducible polynomial $q(x)$ give different circuits, among which the one with shortest length is chosen. There is no apparant way to know the $q(x)$ directly from the sequence which gives the shortest length circuit.

In the light of the work done in this thesis, following points need further investigation.

1. Amounts of shifts $\beta_2, \beta_3 \ldots \beta_n$ for the rows of a maximal sequence are integral multiples of a number β which can be calculated in terms of m and n. But can β_i be known directly from the knowledge of β and the connection polynomial $\underline{\underline{C}}(d)$, without calculating the product $[\underline{\underline{C}}(d)]^{-1}\underline{P}(d)$? If yes, then the sequence generated by a primitive polynomial $\underline{\underline{C}}(d)$ can be obtained directly by taking the sequence generated by

det $[\underline{\underline{C}}(d)]$ as the first row (which can be seen from some table) and then writing the other rows using β_i.

(2) Among the primitive polynomials $\underline{\underline{I}} + \sum_{i=1}^{m} \underline{\underline{C}}_i 2^j d^i$, $j=0,1,2...n-1$, which one gives minimum β_i, so that for others, amounts of shifts are $2^j.\beta_i$?

(3) For a given sequence over $GF(2^n)$, can a $q(x)$ be known which gives the shortest length LFSR circuit, without synthesizing it for all possible choices of $q(x)$?

REFERENCES

1. Huffman, D.A., ''The Synthesis of Linear Sequential Coding Networks''. Information Theory ed. Colin Cherry, New York: Academic Press, 1956.

2. Kautz, W.H., ed. ''Linear Sequential Switching Circuits''. Selected Technical Papers. Holden-Day, Inc. 1965.

3. Elpas, B., ''The Theory of Autonomous Linear Sequential Networks''. IRE Trans. CT-6, 1959, pp. 45-60.

4. Hartmanis, J., ''Linear Multivalued Sequential Coding Networks''. IRE Trans., CT-6, 1959, pp. 69-74.

5. Savage, J.E., ''Some Simple Self-Synchsonising Digital Data Scramblers''. The B.S.T.J., Feb. 1967, pp.449-487.

6. Friedland, B., and Stern, T.E., ''On Periodicity of States in Linear Modulaer Sequential Circuits''. IRE Trans. CT-6, 1959, pp. 61-68.

7. Nakamura, K. and Idawere, et. al., ''Data Scramblers for for Multilevel Pulse Sequences''. Electronics and Communication in Japan, Vol. 55-A, No. 6, 1972, pp 18.

8. Massey, J.L., ''Shift Register Synthesis and BCH Decoding''. IEEE Trans., IT-15, No. 1, 1969, pp 122-127.

9. Peterson, W.W. and Weldon, L.J. Jr., ''Error Correcting Codes''. 2nd ed., The MIT Press, Cambridge, Mass. 1971.

10. Sreedhar, M.N., ''Periodic Response and Spectral Analysis of Digital Data Scramblers''. M. Tech. Thesis, Deptt. of Elect. Engg., Indian Institute of Technology, Kanpur, 1982.

11. Kasai, H., et. al., ''PCM Jitter Suppression by Scrambling'' IEEE Trans., COM-22, Aug. 1974, pp 1114-1122.

12. Yaralagadda, R.B., ''Synchromisation of M-Sequences''. Electronic Letters, 21 Jan. 1982, Vol. 18, No. 2, pp 68-69.

13. Geffe, P.R., ''An Open Letter to Communication Engineers''. Proc. IEEE, Vol. 55, 1967, pp 2173.

14. Manolarakis, M. and Kalouptsidis, N., ''Sequences of Linear Feedback Shift Registers with Nonlinear Feedrorward Logic''. IEEE Proc.E, Vol. 130, Part E, No. 5, Sept. 1983, pp 174-176.

15. Forney, G.D., Jr., ''On Decoding BCH Codes''. IEEE Trans. IT-11, 1965, pp 549-557.

16. Chien, R.T., ''Cyclic Decoding Procedures for BCH Codes''. IEEE Trans., IT-10, 1964, pp 357-363.

17. Berlekamp, E.R., ''Algebraic Coding Theory''. New York: McGraw-Hill Book Co. 1968.

18. Herstein, ''Topics in Algebra''.

19. Birkhoff, G. and S. Mac Lane, ''A Survey of Modern Algebra''. New York: The McMillan Co. 1941.

20. Feher, Digital Communications and Microwave Applications''.

21. Blahut, R.E., ''Theory and Practice of Error Control Codes''. New York: Addison-Wesley Publishing Co., Inc. 1983.

Appendix A

Inverse of the connection polynomial $\underline{\underline{C}}(d)$ over $GF(2^n)$

The polynomial $\underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{C}}_1 d + \underline{\underline{C}}_2 d^2 + \ldots + \underline{\underline{C}}_m d^m$ is the connection polynomial of some LFSR circuit over $GF(2^n)$ and therefore is a polynomial over $GF(2^n)$.

Therefore by the definition of exponent of a polynomial, we conclude that $\underline{\underline{C}}(d)$ is a factor of $\underline{\underline{I}}(1+d^2)$ for some least integer L.

$$\therefore \quad \underline{\underline{C}}(d) = \text{factor of } \underline{\underline{I}}(1+d^2)$$

$$\therefore \quad \underline{\underline{C}}(d)\, \underline{\underline{C}}''(d) = \underline{\underline{I}}(1+d^2)$$

$$\therefore \quad \underline{\underline{C}}''(d) = [\underline{\underline{C}}(d)]^{-1}\, \underline{\underline{I}}(1+d^2)$$

$$\text{or} \quad [\underline{\underline{C}}(d)]^{-1} = \frac{\underline{\underline{C}}''(d)}{1+d^2} \qquad \text{(A.1)}$$

where $\underline{\underline{C}}''(d)$ is also a polynomial over $GF(2^n)$.

Since $\underline{\underline{C}}(d)$ is a n x n matrix with polynomials over GF(2) as its entries, we can write

$$\underline{\underline{C}}(d) = \begin{bmatrix} C_{11}(d) & C_{12}(d) & \ldots & C_{1n}(d) \\ C_{21}(d) & C_{22}(d) & \ldots & C_{2n}(d) \\ \vdots & \vdots & & \\ C_{n1}(d) & C_{n2}(d) & \ldots & C_{nn}(d) \end{bmatrix}$$

$$\therefore [\underline{\underline{C}}(d)]^{-1} = \begin{bmatrix} C'_{11}(d) & C'_{12}(d) & \ldots & C'_{1n}(d) \\ C'_{21}(d) & C'_{22}(d) & \ldots & C'_{2n}(d) \\ \vdots & & & \\ C'_{n1}(d) & C'_{n2}(d) & \ldots & C'_{nn}(d) \end{bmatrix} \cdot \frac{1}{N(d)}$$

where $C'_{ij}(d)$ = cofactor of $C_{ji}(d)$ in $\underline{\underline{C}}(d)$

and $N(d)$ = Determinant of $\underline{\underline{C}}(d)$

Therefore

$$[\underline{\underline{C}}(d)]^{-1} = [\underline{\underline{C}}'(d)] \frac{1}{N(d)} \qquad (A2)$$

In otherwords, inverse of $\underline{\underline{C}}(d)$ can be determined by considering $\underline{\underline{C}}(d)$ as a matrix and applying ordinary matrix inversion technique.

Example A.1. The connection polynomial of a LFSR circuit over $GF(2^3)$ is $\underline{I} + \underline{\alpha}\, d + \underline{\alpha}^2 d + \underline{\alpha}^6 d^3$

where $\underline{\alpha} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ is the primitive element of $GF(2^3)$ and $q(x) = 1+x+x^3$. Find

$$\underline{\underline{C}}(d) \text{ and } [\underline{\underline{C}}(d)]^{-1}$$

Here $$\underline{\underline{M}} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Matrix corresponding to $\underline{\alpha}$ is $\underline{\underline{\alpha}} = [\underline{\alpha}\ \underline{\underline{M}}\underline{\alpha}\ \ \underline{\underline{M}}^2\underline{\alpha}] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

$$\underline{\underline{\alpha}}^2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} ; \quad \underline{\underline{\alpha}}^6 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{\alpha}}\, d + \underline{\underline{\alpha}}^2 d^2 + \underline{\underline{\alpha}}^6 d^3$$

$$\begin{bmatrix} 1+d^3 & d^2+d^3 & d \\ d & 1+d^2 & d+d^2+d^3 \\ d^2+d^3 & d & 1+d^2 \end{bmatrix}$$

$$\therefore \quad [\underline{\underline{C}}(d)]^{-1} = \begin{bmatrix} 1+d^2+d^3 & d^3+d^4+d^5 & 1+d^6 \\ 1+d^6 & 1+d^2+d^4+d^5 & 1+d^3+d^4+d^5+d^6 \\ d^3+d^4+d^5 & 1+d^6 & 1+d^2+d^4+d^5 \end{bmatrix}$$

$$\times \frac{1}{1+d^3+d^4+d^8+d^9}$$

and therefore $N(d) = 1+d^3+d^4+d^8+d^9$.

Appendix B

Exponent of $\underline{\underline{C}}(d)$

From Eq. A.1, the exponent of $\underline{\underline{C}}(d)$ is L.

Consider Eq. A.2. Suppose exponent of N(d) is L'. Then

$$[\underline{\underline{C}}(d)]^{-1} = [\underline{\underline{C}}'(d)] \frac{1}{N(d)} = [\underline{\underline{C}}'(d)] \frac{N'(d)}{1+d^{L'}} .$$

$\therefore$ If $L < L'$ then

$[\underline{\underline{C}}(d)]$ is a factor of $\underline{\underline{I}}(1+d^L)$

$\det[\underline{\underline{C}}(d)]$ is a factor of $\det[\underline{\underline{I}}(1+d^2)]$

$N(d)$ is a factor of $(1+d^2)$

Exponent of N(d) is least $(L, L') = L$ and not L'.

If $L > L'$ then

$$[\underline{\underline{C}}(d)]^{-1} = [\underline{\underline{C}}'(d)] \frac{N'(d)}{1+d^{L'}} = \frac{[\underline{\underline{C}}'(d)\ N'(d)]}{1+d^{L'}}$$

or $[\underline{\underline{C}}(d)][\underline{\underline{C}}'(d)\ N'(d)] = \underline{\underline{I}}(1+d^{L'})$

i.e. $\underline{\underline{C}}''(d)$ is a factor of $\underline{\underline{I}}(1+d^{L'})$

Exponent of $\underline{\underline{C}}(d) = L'$

Therefore if $L \neq L'$ then Exp. $[N(d)] = \text{Exp}\,[\underline{\underline{C}}(d)]$.

In otherwords, exponent of $\underline{\underline{C}}(d)$ is same as the exponent of its determinant $N(d)$.

Example B.1. The determinant of $\underline{\underline{C}}(d) = \underline{\underline{I}} + \underline{\underline{\alpha}}d + \underline{\underline{\alpha}}d^2$ over $GF(2^2)$ is $1+d+d^4$, where $\underline{\underline{\alpha}} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ is element of $GF(2^2)$.

$\underline{\underline{C}}(d)$ is a factor of $\underline{\underline{I}}(1 + d^L)$ with least value of $L=15$.

Also $1+d+d^4$ is a factor of $1+d^{L'}$ with least value of $L' = 15$. Therefore $L = L'$ i.e.

$$\text{Exp}\,[\,\underline{\underline{C}}(d)] = \text{Exp}\,[N(d)] = \text{Exp}\,[\det\{\underline{\underline{C}}(d)\}].$$

Appendix C

$$\text{Exp}\,[q(d^{\beta})] = \beta(\text{Exp}\,[q(d)])$$

Let $q(d) = q_o + q_1 d + q_2 d^2 + \ldots + q_n d^n$ is a polynomial with exponent e. We have to prove that for

$q(d^{\beta}) = q_o + q_1 d^4 + q_2 d^{2\beta} + \ldots + q_n d^{n\beta}$ the exponent is $\beta.e$

Assume on contrary that exponent of $q(d^{\beta})$ is $f < \beta e$

$q(d^{\beta})$ divides $1+d^f$

Put $d^{\beta} = x$

$q(x)$ divides $1+x^{f/\beta}$

Exponent of $q(x) = f/\beta < e$ which is contradiction to the statement that exponent of $q(x) = e$

Assumption is wrong

$f = \beta e$

Exponent of $q(d^{\beta})$ is βe

Example C.1. Let $q(d) = 1+d+d^2+d^5+d^6$

Calculation shows that Exp $[q(d)] = 63$

$$q(d^2) = 1+d^2+d^4+d^{10}+d^{12}$$

Calculation shows that Exp $[q(d^2)] = 126 = 2.$ Exp $[q(d)]$

$$q(d^3) = 1+d^3+d^6+d^{15}+d^{18}$$

Calculation shows that Exp $[q(d^3)] = 189 = 3$ Exp $[q(d)]$

Therefore Exp $[q(d^\beta)] = \beta$ x Exp $[q(d)]$ is verified from this example.

Appendix D

List of factors of polynomials over GF(2)

Weldon and Peterson[9] have given the list of irreducible polynomials over GF(2) and information about the nature of their roots. Here we give the list of all polynomials through degree 8 with their factors over GF(2). Only coefficients of powers of x of the polynomials are given in the list. The corresponding polynomials may be obtained as is clear from the following example. The symbols N and P mean irreducible and primitive respectively.

Example D.1. In the list, factors of 101101011 are 11.1011.11111. The corresponding polynomials are

$$101101011 = 1+x^2+x^3+x^5+x^7+x^8$$

$$11 = 1+x$$

$$1011 = 1+x^2+x^3$$

$$11111 = 1+x+x^2+x^3+x^4$$

$$1+x^2+x^3+x^5+x^7+x^8 = (1+x)\cdot(1+x^2+x^3)\cdot(1+x+x^2+x^3+x^4).$$

POLYNOMIALS	FACTORS			
DEGREE 2				
1 0 1	11	11		
1 1 1	P			
DEGREE 3				
1 0 0 1	11	111		
1 1 0 1	P			
1 0 1 1	P			
1 1 1 1	11	11	11	
DEGREE 4				
1 0 0 0 1	11	11	11	11
1 1 0 0 1	P			
1 0 1 0 1	111	111		
1 0 0 1 1	P			
1 1 1 0 1	11	1011		
1 1 0 1 1	11	11	111	
1 0 1 1 1	11	1101		
1 1 1 1 1	N			
DEGREE 5				
1 0 0 0 0 1	11	11111		
1 1 0 0 0 1	111	1011		
1 0 1 0 0 1	P			
1 0 0 1 0 1	P			
1 0 0 0 1 1	111	1101		
1 1 1 0 0 1	11	11	1101	
1 1 0 1 0 1	11	10011		
1 1 0 0 1 1	11	11	11	11
1 0 1 1 0 1	11	11	11	111
1 0 1 0 1 1	11	11001		
1 0 0 1 1 1	11	11	1011	
1 1 1 1 0 1	P			
1 1 1 0 1 1	P			
1 1 0 1 1 1	P			
1 0 1 1 1 1	P			
1 1 1 1 1 1	11	111	111	
DEGREE 6				
1 0 0 0 0 0 1	11	11	111	111
1 1 0 0 0 0 1	P			
1 0 1 0 0 0 1	1101	1101		
1 0 0 1 0 0 1	N			
1 0 0 0 1 0 1	1011	1011		
1 0 0 0 0 1 1	P			
1 1 1 0 0 0 1	11	101111		
1 1 0 1 0 0 1	11	11	11	1011
1 1 0 0 1 0 1	11	111	1101	
1 1 0 0 0 1 1	11	11	11111	

| | | |

```
1 0 0 1 1 1 0 1        P
1 0 0 1 1 1 1 1        1101          11111
1 0 0 1 0 1 1 1        111           11              1011
1 0 0 0 1 1 1 1        P
1 1 1 1 1 0 1 1        11            1010111
1 1 1 1 0 1 0 1        11            11              111             1011
1 1 1 1 0 0 1 1        11            1101            1101
1 1 1 0 1 1 1 1        11            1011011
1 1 1 0 1 0 1 1        11            11              110111
1 1 1 0 0 1 1 1        11            111             11111
1 1 0 1 1 0 1 1        11            1001001
1 1 0 1 1 0 0 1        11            11              111011
1 1 0 0 1 1 1 1        11            1011            1011
1 0 1 1 1 0 1 1        11            111             111             111
1 0 1 1 1 0 0 1        11            11              11              1011
1 0 1 1 0 1 1 1        11            111             11111
1 0 1 0 1 1 1 1        11            11              111             1101
1 0 0 1 1 1 1 1        11            1110101
1 1 1 1 1 1 0 1        P
1 1 1 1 1 0 1 1        111           100101
1 1 1 1 0 1 1 1        P
1 1 1 0 1 1 1 1        P
1 1 0 1 1 1 1 1        111           101001
1 0 1 1 1 1 1 1        P
1 1 1 1 1 1 1 1        11            11              11              11              11,11,11
```

DEGREE 8

```
1 0 0 0 0 0 0 0 1      11            11              11              11              11,11,11,11
1 1 0 0 0 0 0 0 1      111           1011011
1 0 1 0 0 0 0 0 1      11001         11001
1 0 0 1 0 0 0 0 1      1101          111101
1 0 0 0 1 0 0 0 1      111           111             111             111
1 0 0 0 0 1 0 0 1      1011          101111
1 0 0 0 0 0 1 0 1      10011         10011
1 0 0 0 0 0 0 1 1      111           1101101
1 1 1 0 0 0 0 0 1      11            10111111
1 1 0 1 0 0 0 0 1      11            11              1110101
1 1 0 0 1 0 0 0 1      11            10001111
1 1 0 0 0 1 0 0 1      11            11              11              11001
1 1 0 0 0 0 1 0 1      11            10000011
1 1 0 0 0 0 0 1 1      11            11              1101            1011
1 0 1 1 0 0 0 0 1      11            111             101001
1 0 1 0 1 0 0 0 1      11            11              1011            1011
1 0 1 0 0 1 0 0 1      11            1101            10011
1 0 1 0 0 0 1 0 1      11            11              11              111             111
1 0 1 0 0 0 0 1 1      11            11000001
1 0 0 1 1 0 0 0 1      11            11101111
1 0 0 1 0 1 0 0 1      11            11              111             11111
1 0 0 1 0 0 1 0 1      11            1011            11001
1 0 0 1 0 0 0 1 1      11            11              11              11              10011
1 0 0 0 1 1 0 0 1      11            11110111
1 0 0 0 1 0 1 0 1      11            11              1101            1101
1 0 0 0 1 0 0 1 1      11            11110001
1 0 0 0 0 1 1 0 1      11            111             100101
1 0 0 0 0 1 0 1 1      11            11              1010111
1 0 0 0 0 0 1 1 1      11            11111101
1 1 1 1 0 0 0 0 1      1011          110111
1 1 1 0 1 0 0 0 1      10011         11111
1 1 1 0 0 1 0 0 1      111           1000011
1 1 1 0 0 0 1 0 1      1101          101001
1 1 1 0 0 0 0 1 1      P
1 1 0 1 1 0 0 0 1      N
```

```
1 1 0 1 0 1 0 0 1        p
1 1 0 1 0 0 1 0 1        111          1010111
1 1 0 1 0 1 0 1 1        p
1 1 0 0 1 1 0 0 1        1101         100101
1 1 0 0 1 0 1 0 1        1011         111011
1 1 0 0 1 0 0 1 1        111          111          11111
1 1 0 0 0 1 1 0 1        p
1 1 0 0 0 1 0 1 1        p
1 1 0 0 0 0 1 1 1        p
1 0 1 1 1 0 0 0 1        p
1 0 1 1 0 1 0 0 1        p
1 0 1 1 0 0 1 0 1        p
1 0 1 1 0 0 0 1 1        p
1 0 0 1 1 0 1 0 1        111          1110011
1 0 0 1 1 0 0 1 1        11111        11111
1 0 0 1 0 1 0 0 1        1101         110111
1 0 0 1 0 1 0 1 1        p
1 0 0 1 0 0 1 1 1        111          1110101
1 0 0 0 1 0 1 1 1        1011         100101
1 0 0 0 1 1 1 0 1        p
1 0 0 0 1 1 0 1 0 1      111          1100111
1 0 0 0 1 1 0 0 1 1      1011         101001
1 0 0 0 1 0 1 1 0 1      p
1 0 0 0 1 0 1 0 1 1      p
1 0 0 0 1 0 0 1 1 1      111          1100001
1 0 0 0 0 1 1 1 0 1      p
1 0 0 0 0 1 1 0 1 1      N
1 0 0 0 0 1 0 1 1 1      11001        11111
1 0 0 0 0 0 1 1 1 1      1101         111011
1 1 1 1 1 1 0 0 0 1      11           11           11           1101
1 1 1 1 0 1 0 0 0 1      11           10100111
1 1 1 1 0 0 1 0 0 1      11           11           1100001
1 1 1 1 0 0 0 1 1 1      11           111          111011
1 1 1 0 1 1 0 0 0 1      11           11           1101101
1 1 1 0 1 0 1 0 0 1      11           111          111101
1 1 1 0 1 0 0 1 1 1      11           11           100101
1 1 1 0 0 1 1 0 0 1      11           11           11           11           101
1 1 1 0 0 1 0 1 1 1      11           10111001
1 1 1 0 0 0 1 1 1 1      11           11           111          111          111
1 1 0 1 1 1 0 0 0 1      11           111          111          1011
1 1 0 1 1 0 1 0 0 1      11           11           11           101111
1 1 0 1 1 0 0 1 1 1      11           10010001
1 1 0 1 0 1 1 0 0 1      11           1101         11111
1 1 0 1 0 1 0 1 1 1      11           11           11           11           11, 11 , 111
1 1 0 1 0 0 1 1 1 1      11           10011101
1 1 0 0 1 1 1 0 0 1      11           11           111          10011
1 1 0 0 1 1 0 1 1 1      11           10001001
1 1 0 0 1 0 1 1 1 1      11           11           11           101001
1 1 0 0 0 1 1 1 1 1      11           111          110111
1 0 1 1 1 1 0 0 0 1      11           11           11           111011
1 0 1 1 1 0 1 0 0 1      11           11010011
1 0 1 1 1 0 0 1 1 1      11           11           111          11001
1 0 1 1 0 1 1 0 0 1      11           11           1001001
1 0 1 1 0 1 0 1 1 1      11           1011         11111
1 0 1 1 0 0 1 1 1 1      11           11           11           11           11           110
1 0 1 0 1 1 1 0 0 1      11           11001011
1 0 1 0 1 1 0 1 1 1      11           11           11           111101
1 0 1 0 1 0 1 1 1 1      11           111          101111
1 0 1 0 0 1 1 1 1 1      11           11           1000011
1 0 0 1 1 1 1 0 0 1      11           11           11           11011
1 0 0 1 1 1 0 1 1 1      11           111          111          1101
1 0 0 1 1 0 1 1 1 1      11           11           1011011
1 0 0 1 0 1 1 1 1 1      11           11100101
1 0 0 0 1 1 1 1 1 1      11           11           11           111          1011
```

1	1	1	1	1	1	0	0	1	S				
1	1	1	1	1	0	1	0	1	P				
1	1	1	1	1	0	0	1	1	A				
1	1	1	1	0	1	1	0	1	111	111	11001		
1	1	1	1	0	1	0	1	1	1101	101111			
1	1	1	1	0	0	1	1	1	P				
1	1	1	0	1	1	1	0	1	R				
1	1	1	0	1	1	0	1	1	111	1011	1011		
1	1	1	0	1	0	1	1	1	I				
1	1	1	0	0	1	1	1	1	N				
1	1	0	1	1	1	1	0	1	T				
1	1	0	1	1	1	0	1	1	11001	10011			
1	1	0	1	1	0	1	1	1	111	1101	1101		
1	1	0	1	0	1	1	1	1	1011	111101			
1	1	0	0	1	1	1	1	1	N				
1	0	1	1	1	1	1	0	1	111	1101	1011		
1	0	0	1	1	1	1	1	1	I				
1	0	0	1	1	1	0	1	1	N				
1	0	0	1	1	0	1	1	1	111	111	10011		
1	0	0	1	0	1	1	1	1	P				
1	0	0	0	1	1	1	1	1	N				
1	1	1	1	1	1	1	0	1	11	10101011			
1	1	1	1	1	1	0	1	1	11	11	1100111		
1	1	1	1	1	0	1	1	1	11	1011	10011		
1	1	1	1	0	1	1	1	1	11	11	11	11	11111
1	1	1	0	1	1	1	1	1	11	1101	11001		
1	1	0	1	1	1	1	1	1	11	11	1110011		
1	0	1	1	1	1	1	1	1	11	11010101			
1	1	1	1	1	1	1	1	1	111	1001001			

****

Appendix E

List of factors of polynomials over $GF(2^2)$

Factors of polynomials over $GF(2^2)$ through degree 4 are listed here. 'a' denotes the element of $GF(2^2)$ corresponding to the vector $\begin{bmatrix}0\\1\end{bmatrix}$ and $q(x) = 1+x+x^2$. 'N' mean irreducible and 'P' means primitive.

Example E.1. Find factors of $\underline{1}+\underline{a}^2x^2+\underline{1}x^4$, $\underline{a} = \begin{bmatrix}0\\1\end{bmatrix}$; $q(x) = 1+x+x^2$

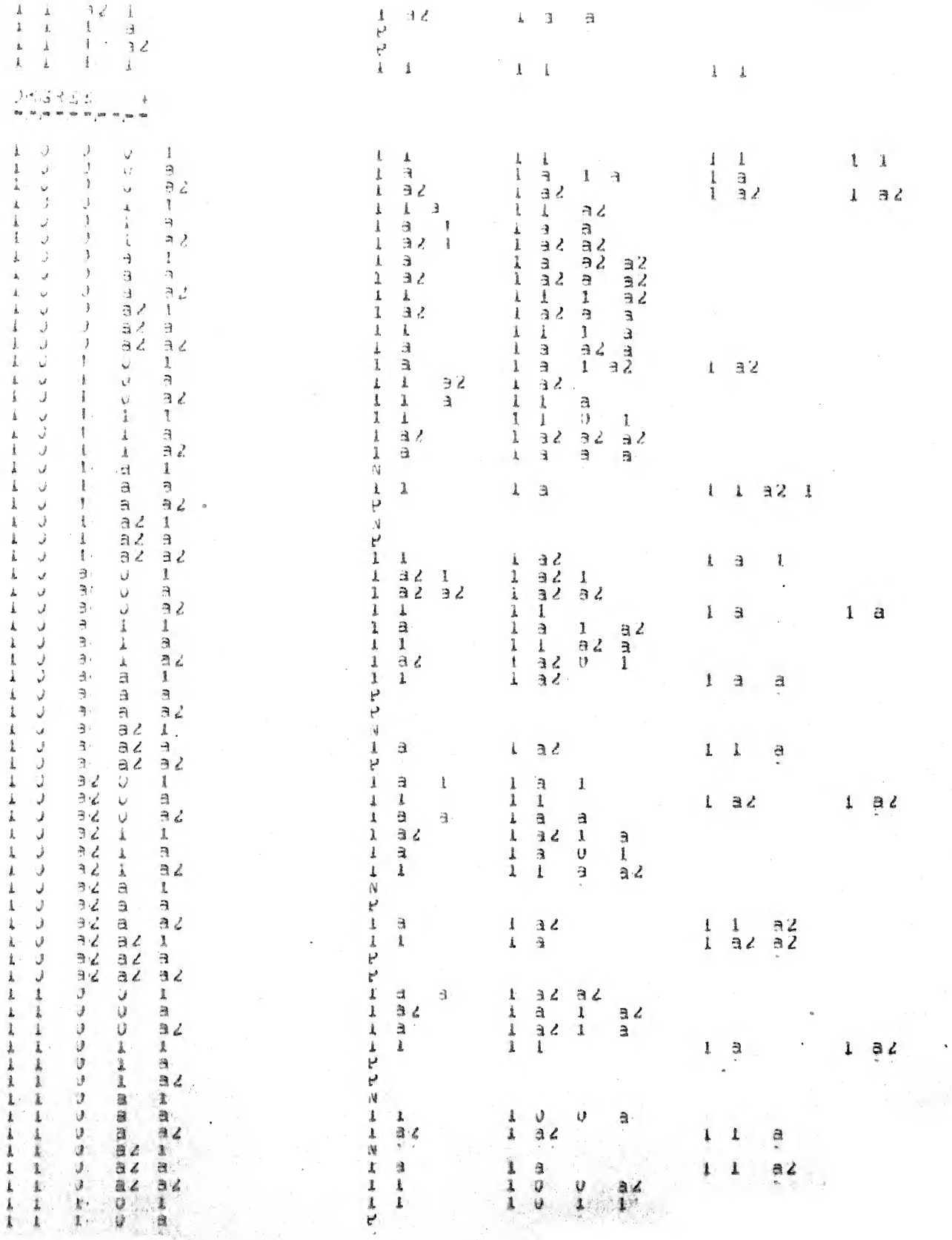
$\underline{1}+\underline{a}^2x^2+\underline{1}x^4$ corresponds to $10a^201$

Factors from table are 1a1 , 1a1

$\therefore\ \underline{1}+\underline{a}^2x^2+\underline{1}x^4 = (\underline{1}+\underline{a}x + \underline{1}x^2)\cdot(\underline{1}+\underline{a}x + \underline{1}x^2)$

Note:- because of the inconvinience in typing powers of 'a', 'a-square' is written as 'a2'.

POLYNOMIALS	FACTORS
DEGREE 2	
1 0 a	1 a2 1 a2
1 0 a2	1 a 1 a
1 0 1	1 1 1 1
1 a a	P
1 a a2	1 1 1 a2
1 a 1	I
1 a2 a	1 1 1 a
1 a2 a2	P
1 a2 1	I
1 1 a	D
1 1 a2	D
1 1 1	1 a 1 a2
DEGREE 3	
1 0 0 a	N
1 0 0 a2	N
1 0 0 1	1 1 1 a 1 a2
1 0 a a	1 a 1 a 1
1 0 a a2	1 1 1 1 a2
1 0 a2 a	N
1 0 a2 a2	1 a2 1 a2 1
1 0 a2 1	N
1 0 1 a	1 a2 1 a2 a2
1 0 1 a2	1 a 1 a a
1 0 1 1	N
1 a 0 a	1 a2 1 1 a2
1 a 0 a2	1 1 1 a2 a2
1 a 0 1	N
1 a a a	D
1 a a a2	1 a 1 a2 1 a2
1 a a 1	1 1 1 a2 1
1 a a2 a	D
1 a a2 a2	D
1 a a2 1	1 a 1 a 1 a
1 a 1 a	1 1 1 1 1 a
1 a 1 a2	P
1 a 1 1	1 a2 1 1 a
1 a2 0 a	1 1 1 a a
1 a2 0 a2	1 a 1 1 a
1 a2 0 1	N
1 a2 a a	D
1 a2 a a2	D
1 a2 a 1	1 a2 1 a2 1 a2
1 a2 a2 a	1 a 1 a 1 a2
1 a2 a2 a2	P
1 a2 a2 1	1 1 1 a 1
1 a2 1 a	P
1 a2 1 a2	1 1 1 1 1 a2
1 a2 1 1	1 a 1 1 a2
1 1 0 a	1 a 1 a2 1
1 1 0 a2	1 a2 1 a 1
1 1 0 1	N
1 1 a a	1 1 1 a2 1 a2
1 1 a a2	P
1 1 a 1	1 a 1 a2 a2
1 1 a2 a	P
1 1 a2 a2	1 1 1 a 1 a



```
1 1 1 0 a2
1 1 1 1 1
1 1 1 1 a
1 1 1 1 a2
1 1 1 a 1
1 1 1 a a
1 1 1 a a2
1 1 1 a2 1
1 1 1 a2 a
1 1 1 a2 a2
1 1 a 0 1
1 1 a 0 a
1 1 a 0 a2
1 1 a 1 1
1 1 a 1 a
1 1 a 1 a2
1 1 a a 1
1 1 a a a
1 1 a a a2
1 1 a a2 1
1 1 a a2 a
1 1 a a2 a2
1 1 a2 0 1
1 1 a2 0 a
1 1 a2 0 a2
1 1 a2 1 1
1 1 a2 1 a
1 1 a2 1 a2
1 1 a2 a 1
1 1 a2 a a
1 1 a2 a a2
1 1 a2 a2 1
1 1 a2 a2 a
1 1 a2 a2 a2
1 a 1 0 1
1 a 1 0 a
1 a 1 0 a2
1 a 1 1 1
1 a 1 1 a
1 a 1 1 a2
1 a 1 a 1
1 a 1 a a
1 a 1 a a2
1 a 1 a2 1
1 a 1 a2 a
1 a 1 a2 a2
1 a a 0 1
1 a a 0 a
1 a a 0 a2
1 a a 1 1
1 a a 1 a
1 a a 1 a2
1 a a a 1
1 a a a a
1 a a a a2
1 a a a2 1
1 a a a2 a
1 a a a2 a2
```

```
P
1 a 1 1 a2 1
1 a 1 a2 0 1
1 a2 1 a 0 1
1 a2 1 a2 1 1 a2
P
1 1 1 a 1 a a
1 a 1 a 1 1 a
1 1 1 a2 1 a2 a2
P
1 a2 1 a a2 a
1 1 1 a 1 a 1
P
1 a2 1 a a2 a2
1 1 1 1 1 1 a2
1 a 1 a2 a2 a2
P
1 1 1 0 a 1
1 a2 1 1 a a
1 a 1 a2 1 a2
1 a 1 a2 a a2
P
1 1 1 a2 1 a2 1
N
1 1 1 1 1 a a
1 a 1 a2 a2
1 1 1 0 a2 1
1 a 1 a 1 a2
1 a2 1 a a a
N
1 1 1 a 1 a 1 a2
P
1 1 1 1 1 a 1
P
1 a 1 0 0 a
1 a 1 0 0 a2
P
1 a2 1 a2 1 a a
N
1 1 1 a2 a a
1 a 1 a2 1 a2 a2
1 a 1 a2 a2 a2
N
1 1 1 a 1 a 1 a2
P
1 1 1 1 1 a2 1 a2
1 a 1 0 1 1
1 1 a2 1 a2 1
1 1 1 a 1 1 a2
1 a2 1 1 1 a2
P
1 a2 1 1 1 a
N
1 a 1 a 1 a 1
1 1 a 1 a2 a2
1 a 1 0 a 1
1 1 1 1 1 1 a2
1 a2 1 a
N
```

```
P
1 a 1 1 a2 1
1 a 1 a2 0 1
1 a2 1 a 0 1
1 a2 1 a2 1 1 a2
P
1 1 1 a 1 a a
1 a 1 a 1 1 a
1 1 1 a2 1 a2 a2
P
1 a2 1 a a2 a
1 1 1 a 1 a 1
P
1 a2 1 a a2 a2
1 1 1 1 1 1 a2
1 a 1 a2 a2 a2
P
1 1 1 0 a 1
1 a2 1 1 a a
1 a 1 a2 1 a2
1 a 1 a2 a a2
P
1 1 1 a2 1 a2 1
N
1 1 1 1 1 a a
1 a 1 a2 a2
1 1 1 0 a2 1
1 a 1 a 1 a2
1 a2 1 a a a
N
1 1 1 a 1 a 1 a2
P
1 1 1 1 1 a 1
P
1 a 1 0 0 a
1 a 1 0 0 a2
P
1 a2 1 a2 1 a a
N
1 1 1 a2 a a
1 a 1 a2 1 a2 a2
1 a 1 a2 a2 a2
N
1 1 1 a 1 a 1 a2
P
1 1 1 1 1 a2 1 a2
1 a 1 0 1 1
1 1 a2 1 a2 1
1 1 1 a 1 1 a2
1 a2 1 1 1 a2
P
1 a2 1 1 1 a
N
1 a 1 a 1 a 1
1 1 a 1 a2 a2
1 a 1 0 a 1
1 1 1 1 1 1 a2
1 a2 1 a
N
```

Appendix F

List of factors of polynomials over $GF(2^3)$

Factors of polynomials over $GF(2^3)$ through degree 3 are listed below. 'a' denotes the element of $GF(2^3)$ corresponding to the vector $\begin{bmatrix}0\\1\\0\end{bmatrix}$ and $q(x) = 1+x+x^3$. 'N' means irreducible.

Example F.1. Find factors of $\underline{1}+\underline{a}^6x + \underline{a}^2x^2$

$\underline{1}+\underline{a}^6x + \underline{a}^2x^2$ is written in the list as $1a^6a^2$. Factors are given to be $11, 1a^2$

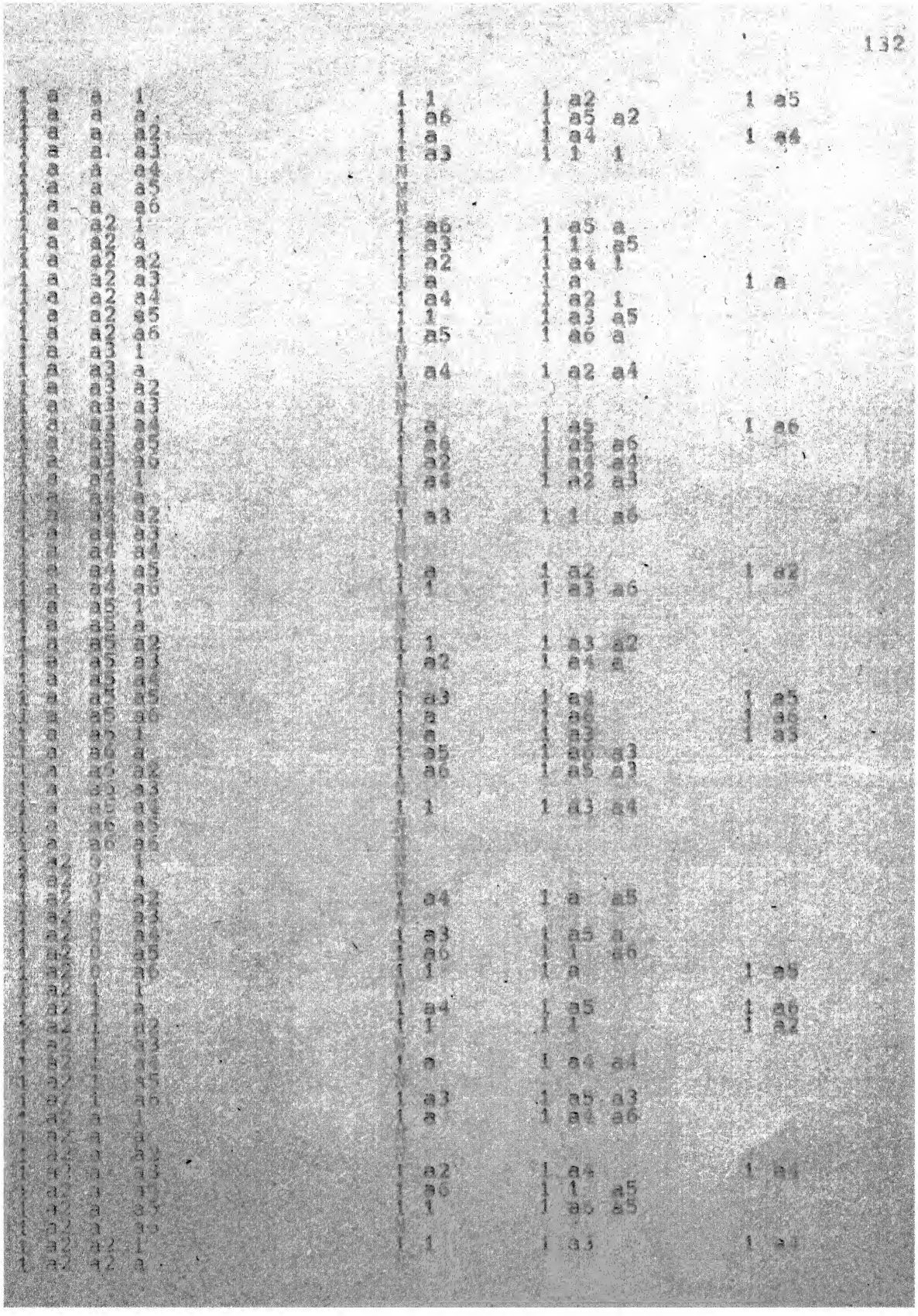
$\therefore \quad \underline{1}+\underline{a}^6x + \underline{a}^2x^2 = (\underline{1}+\underline{1}x)\cdot(\underline{1}+\underline{a}^2x)$.

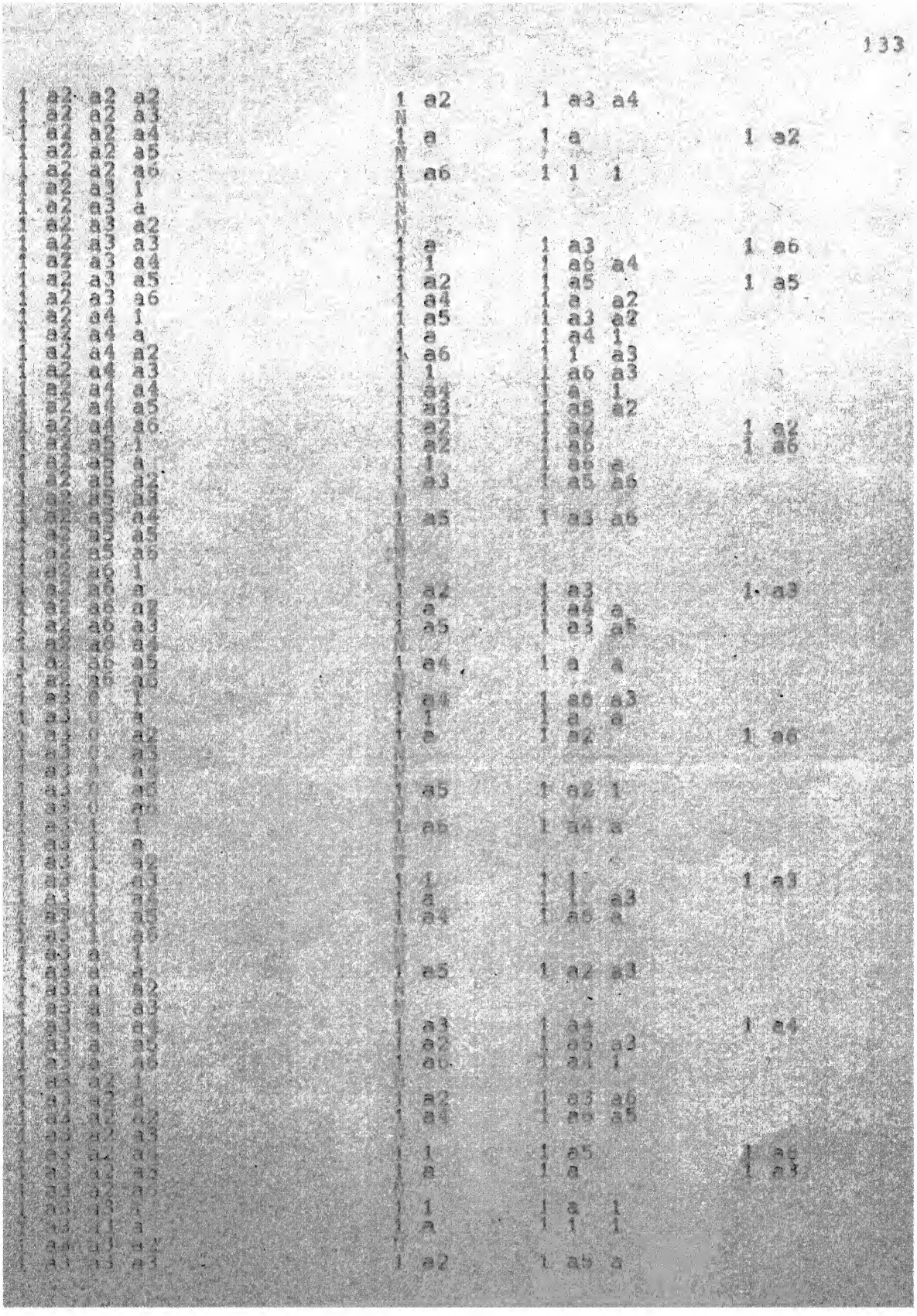
NOTE:- Because of the inconvinience in typing powers of 'a', 'a-squared', 'a-cubed',..... 'a-power 6' are written as 'a2', 'a3',..... 'a6'.

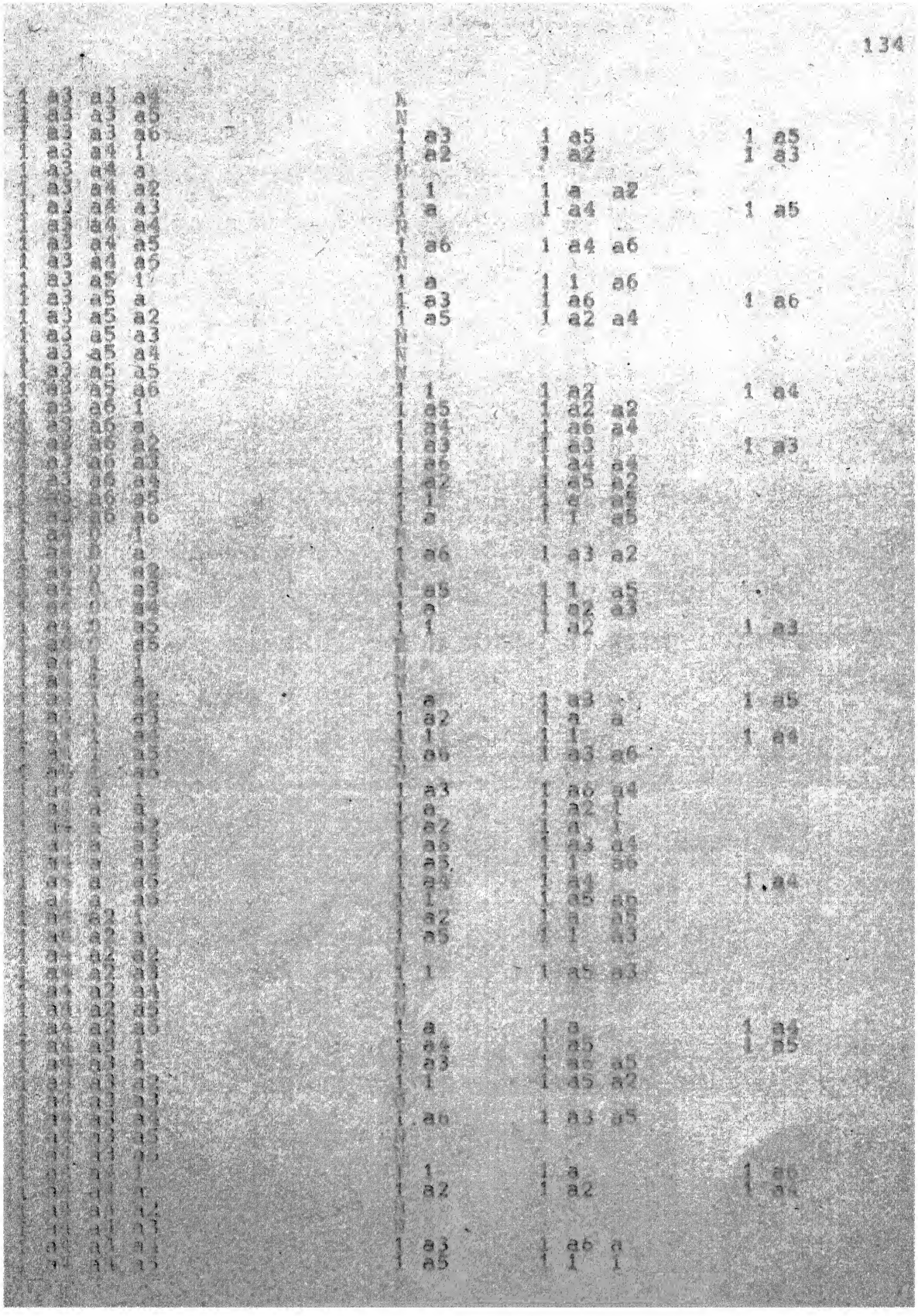
POLYNOMIALS	FACTORS
DEGREE 2	
1 0 1	1 1 1 1
1 0 a	1 a4 1 a4
1 0 a2	1 a 1 a
1 0 a3	1 a5 1 a5
1 0 a4	1 a2 1 a2
1 0 a5	1 a6 1 a6
1 0 a6	1 a3 1 a3
1 1 1	N
1 1 a	1 a2 1 a6
1 1 a2	1 a4 1 a5
1 1 a3	P
1 1 a4	1 a 1 a3
1 1 a5	P
1 1 a6	P
1 a 1	P
1 a a	P
1 a a2	P
1 a a3	1 1 1 a3
1 a a4	1 a5 1 a6
1 a a5	P
1 a a6	1 a2 1 a4
1 a2 1	P
1 a2 a	1 a3 1 a5
1 a2 a2	P
1 a2 a3	P
1 a2 a4	P
1 a2 a5	1 a 1 a4
1 a2 a6	1 1 1 a6
1 a3 1	1 a2 1 a5
1 a3 a	1 1 1 a
1 a3 a2	P
1 a3 a3	1 a4 1 a6
1 a3 a4	P
1 a3 a5	P
1 a3 a6	P
1 a4 1	P
1 a4 a	P
1 a4 a2	1 a3 1 a6
1 a4 a3	1 a 1 a2
1 a4 a4	P
1 a4 a5	1 1 1 a5
1 a4 a6	P
1 a5 1	1 a 1 a6
1 a5 a	P
1 a5 a2	P
1 a5 a3	P
1 a5 a4	1 1 1 a4
1 a5 a5	1 a2 1 a3
1 a5 a6	P
1 a6 1	1 a3 1 a4
1 a6 a	P
1 a6 a2	1 1 1 a2
1 a6 a3	P
1 a6 a4	P
1 a6 a5	P
1 a6 a6	1 a 1 a5

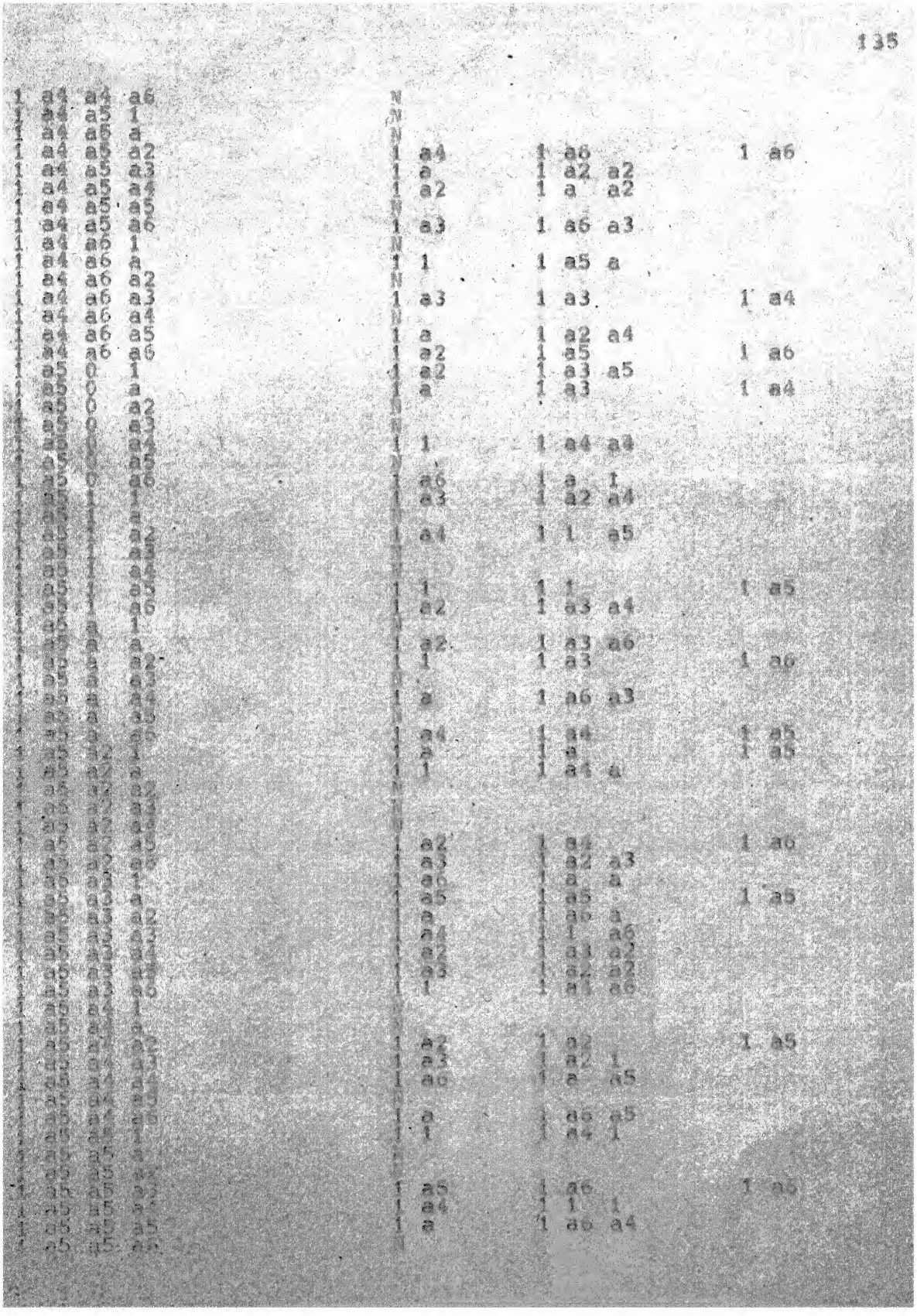
DEGREE 3

| | | |









```
1 a5 a6 1          1 a4       1 1  a3
1 a5 a6 a          1 a6       1 a  a2
1 a5 a6 a2         N
1 a5 a6 a3         1 1        1 a          1 a2
1 a5 a6 a4         1 a3       1 a3         1 a5
1 a5 a6 a5         N
1 a5 a6 a6         N
1 a6 0  1          1 a        1 a5 a6
1 a6 0  a          1 1        1 a2 a2
1 a6 0  a2         N
1 a6 0  a3         1 a3       1 a4 1
1 a6 0  a4         1 a2       1 a4         1 a5
1 a6 0  a5         N
1 a6 0  a6         N
1 a6 1  1          1 a5       1 a  a2
1 a6 1  a          1 a2       1 1  a6
1 a6 1  a2         N
1 a6 1  a3         1 a        1 a3 a2
1 a6 1  a4         N
1 a6 1  a5         N
1 a6 1  a6         1 1        1 1          1 a6
1 a6 a  1          1 a4       1 a4         1 a6
1 a6 a  a          N
1 a6 a  a2         N
1 a6 a  a3         1 a5       1 a  a5
1 a6 a  a4         1 1        1 a2 a4
1 a6 a  a5         N
1 a6 a  a6         1 a        1 a2         1 a3
1 a6 a2 1          N
1 a6 a2 a          1 a        1 a          1 a6
1 a6 a2 a2         1 a3       1 a4 a6
1 a6 a2 a3         1 a4       1 a3 a6
1 a6 a2 a4         N
1 a6 a2 a5         1 a5       1 a  1
1 a6 a2 a6         N
1 a6 a3 1          1 a2       1 1  a5
1 a6 a3 a          N
1 a6 a3 a2         1 a6       1 a5         1 a6
1 a6 a3 a3         N
1 a6 a3 a4         1 a3       1 a4 a
1 a6 a3 a5         1 1        1 a          1 a4
1 a6 a3 a6         N
1 a6 a4 1          N
1 a6 a4 a          1 1        1 a3         1 a5
1 a6 a4 a4         1 a4       1 a3 a5
1 a6 a4 a3         1 a2       1 a2         1 a6
1 a6 a4 a4         1 a        1 a5 a3
1 a6 a4 a5         N
1 a6 a4 a6         N
1 a6 a5 1          1 a3       1 a4 a4
1 a6 a5 a          1 a4       1 a3 a4
1 a6 a5 a2         1 a        1 a5 a
1 a6 a5 a3         1 1        1 a2 a3
1 a6 a5 a4         1 a6       1 a6         1 a6
1 a6 a5 a5         1 a2       1 1  a3
1 a6 a5 a6         1 a5       1 a  a
1 a6 a6 1          1 1        1 a2 1
1 a6 a6 a          N
1 a6 a6 a2         1 a2       1 1  1
1 a6 a6 a3         N
1 a6 a6 a4         N
1 a6 a6 a5         1 a3       1 a3         1 a6
1 a6 a6 a6         1 a4       1 a6 a2
```